Intellectual Property and Internet Litigation: Law and Developing Trends

The Computer Law Committee of the IP Section of the State Bar of California and Southwestern School of Law

Grokster and the Future of P2P File-sharing

April 15, 2005

Ian C. Ballon
Manatt, Phelps & Phillips, LLP

11355 West Olympic Boulevard
Los Angeles, CA 90064-1614
Direct Dial: (310) 312-4326
Fax: (310) 312-4224

1001 Page Mill Road, Bldg. 2
Palo Alto, CA 94304-1006
Direct Dial: (650) 812-1389
Fax: (650) 213-0260

Iballon@manatt.com
<www.ballononecommerce.com>

An earlier version of this paper was published by the American Bar Association in the book "The Performing Art of Advocacy: Creating A New Spirit" and presented at the 1995 ABA Annual Convention in Chicago, Illinois in conjunction with the program "Litigating in a Cyberspace World." The materials in this outline have been incorporated in the 3 volume set, "E-Commerce and Internet Law: A Legal Treatise With Forms," by Ian C. Ballon, published by Glasser LegalWorks. For information on the legal treatise, contact Glasser LegalWorks at (800) 308-1700 or access the website for the book at www.ballononecommerce.com. The opinions expressed are solely those of the author.

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

I. COPYRIGHT PROTECTION IN CYBERSPACE

A. Statutory Background

1. U.S. copyright law protects original and creative expression, but not underlying ideas.

2. Copyright protection extends to:

   a. Original works of authorship

   b. Fixed in a tangible medium of expression. 17 U.S.C. § 102(a).

      (1) Software is deemed to be "fixed in a tangible medium" even when not stored on disk. MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993) (turning on a computer, which causes the operating system to be loaded from permanent storage to the computer's random access memory (RAM), was held to constitute copyright infringement where the person turning on the computer was not licensed to use the operating system), cert. dismissed, 510 U.S. 1033 (1994); see also Triad Systems Corp. v. Southeastern Express Co., 64 F.3d 1330 (9th Cir. 1995), cert. denied, 516 U.S. 1145 (1996); Advanced Computer Services v. MAI Systems Corp., 845 F. Supp. 356 (E.D. Va. 1994) (same holding). In MAI Systems Corp., the Ninth Circuit wrote that "[t]he representation created in the RAM 'is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.'" 991 F.2d at 518.

      (2) Usenet newsgroup postings. In Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995), Usenet postings of copyrighted works were held to create "copies" under MAI Systems Corp. v. Peak Computer, Inc., supra, (1) when automatically (and briefly) stored on a BBS computer and then (2) when automatically copied to an Internet access provider's computer and then (3) when automatically copied onto other computers on the Usenet. See infra § I(F)(7).

      (3) Browsing. When a user browses the Internet, the act of browsing causes a copy of the digital information viewed on the screen temporarily to be made in the user's computer

screen memory. Under MAI Systems Corp. v. Peak Computer, Inc., supra, a copy is fixed when information is temporarily placed in RAM, including screen RAM. Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361, 1378 n.25 (N.D. Cal. 1995); see infra § I(F)(7).

(4) Interactive works are also deemed to be "fixed in a tangible medium," even though the sequence of action can be altered by each individual user. See Atari Games Corp. v. Oman, 888 F.2d 878, 884 (D.C. Cir. 1989).

3. Copyright protection may be obtained for:

a. Literary works. As a result of the recommendations of the CONTU commission, Congress, in 1980, expressly amended the 1976 Copyright Act to provide that software would be treated as a "literary work." See Apple Computer, Inc. v. Formula Int'l Inc., 725 F.2d 521, 524-25 (9th Cir. 1984).

b. Musical works, including any accompanying words.

c. Dramatic works, including any accompanying music.

d. Pantomimes and choreographic works.

e. Pictorial, graphic and sculptural works.

f. Motion pictures and other audiovisual works. Screen displays, or the user-interface of a computer program, may be entitled to protection as an audiovisual work. See, e.g., Computer Associates Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 703 (2d Cir. 1992).

g. Sound recordings.

h. Architectural works. 17 U.S.C. § 102(a).

4. Exclusions. Copyright protection does not extend to any idea, procedure, process, system, method of operation, concept, principle or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work. 17 U.S.C. § 102(b).

5. Exclusive rights in copyrighted works. A copyright grants the owner the exclusive right to do and authorize any of the following (subject to the first sale doctrine codified at 17 U.S.C. § 109(a), infra § VI(A)(1)):

a. to reproduce the copyrighted work in copies or phonorecords;

b. to prepare derivative works based upon the copyrighted work;

c. to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;

d. in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly;

e. in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; and

f. in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission. 17 U.S.C. § 106.

6. Exception: archival or back-up copies of software and temporary copies created for maintenance or repair. 17 U.S.C. § 117 creates an exception to the exclusive rights granted a copyright owner under 17 U.S.C. § 106 for back-up copies of software programs. Pursuant to a 1998 amendment to the Copyright Act, a narrow exception also exists for temporary copies created "solely by virtue of the activation of a machine that lawfully contains an authorized copy . . . for purposes only of maintenance or repair of that machine . . . ."

B. Derivative Works and Multimedia Clearance

1. Copyright protection in a derivative work or compilation extends only to the material contributed by the author of such work, and does not grant rights in preexisting material included in the new work. 17 U.S.C. § 103.

2. Multimedia and web-based works often are "derivative works." As a result of digital technology, it is today relatively easy to cut and past sound, visual images, text and software applications to create new "works." These works generally would be characterized as "derivative works," because they are based on preexisting works. 17 U.S.C. § 101.

3. Clearance. With multimedia works, it is important to ensure that permission to use each aspect of the work has been obtained. The rights to each prior work incorporated in a derivative multimedia work (i.e., text, motion pictures, software) may be owned by different entities. In addition, since all of the rights granted by a copyright may be separately licensed, different entities may have exclusive licenses to different forms of the same work (i.e., book rights, motion picture rights, etc.). Further,

even an exclusive licensee may not have rights that would extend to a new, multimedia application. Clearance issues therefore can be quite complex and, if not properly addressed, lead to litigation.

4. In Video Pipeline, Inc. v. Buena Vista Home Entertainment, Inc., 342 F.3d 191 (3d Cir. 2003), cert. denied, 124 S. Ct. 1410 (2004), the circuit court affirmed the entry of an injunction prohibiting a website-middleman's creation of its own movie trailers for use by its client video retailers and the online display of clip previews (approximately 2 minute segments) as a violation of the copyright owner's exclusive right to create its own trailers from its motion pictures.

5. Digital technology challenges traditional copyright law. Almost a decade ago, Professor Pamela Samuelson and Robert Glushko identified several characteristics of works in digital form that they foresaw would change the contours of copyright law, including: (1) the ease with which such works can be replicated and the ease with which they can be transmitted and accessed by multiple users "would seem to create strong incentives for copyright industries to move away from their traditional focus of the sale of copies, and toward greater control over uses of protected works"; (2) the ease with which digital works can be manipulated and modified creates new benefits and problems since copyright law is more geared toward dealing with works that are permanently fixed; (3) the breakdown among copyright distinctions among different kinds of works when they are in digital form suggests that the eight categories of protected works (supra § I(A)(3)), each of which has somewhat varying degrees of protection, need to be revised; and (4) the fact that digital works allow new kinds of search and linking activities to be achieved, giving rise to hybrid multimedia works, which the authors characterized as "new classes of protected intellectual property products, including hypertext." Symposium, "Electronic Communications and Legal Change: Intellectual Property Rights for Digital Library and Hypertext Publishing Systems," 6 Harv. J.L. & Tech. 237, 237-40 (1993).

C. Software Infringement

1. What is protectable. The level of creativity required for a work to qualify for copyright protection is extremely low. As explained by the U.S. Supreme Court, "the requisite level of creativity is low; even a slight amount will suffice." Feist Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340, 345 (1991). Despite this low standard, many "minimally creative" or functional aspects of computer programs are not entitled to copyright protection. Although the law in this area is still evolving, and varies in certain respects in the different federal circuit courts, the following are examples of aspects of software programs that may not be entitled to copyright protection:

a. Menu command hierarchies. See Lotus Development Corp. v. Borland Int'l, Inc., 49 F.3d 807 (1st Cir. 1995), aff'd mem., 516 U.S. 233 (1996) (4-4 decision). But see Autoskill Inc. v. National Educational Support Systems, Inc., 994 F.2d 1476 (10th Cir.), cert. denied, 510 U.S. 916 (1993) (*rejecting* the defendant's argument that the keying procedure used in a computer program designed to test and train students with learning deficiencies was an uncopyrightable "procedure" or "method of operation"); see also Lotus v. Borland, 49 F.3d at 819-21 (Boudin, J. concurring) (emphasizing that Lotus' menu commands presented a particularly unattractive case for copyright protection because they "are largely for standard procedures that Lotus did not invent and are common words that Lotus cannot monopolize . . .").

b. Icons. Apple Computer, Inc. v. Microsoft Corp., 35 F.3d 1435, 1443-44 (9th Cir. 1994), cert. denied, 513 U.S. 1184 (1995) (holding unprotectable Apple's "iconic representation of familiar objects from the office environment" and "the manipulation of icons to convey instructions and to control operation of the computer").

c. Use of windows to display multiple images on the computer screen and to facilitate user interaction with the information contained in the windows. Id.

d. Use of menus to store information or computer functions in a place that is convenient to reach, but saves screen space for other images. Id.

e. Opening and closing of objects as a means of retrieving, transferring and storing information. Id.

f. A computer animated key pad. Mitek Holdings, Inc. v. ARCE Engineering Co., 864 F. Supp. 1568, 1581 (S.D. Fla. 1994), aff'd, 89 F.3d 1548 (11th Cir. 1996).

g. Constants. Constants are the invariable integers that comprise part of the formulas used to perform the calculations in certain programs. In Gates Rubber Co. v. Bando Chemical Industries, Ltd., 9 F.3d 823 (10th Cir. 1993), the constants represented scientific observations of physical relationships concerning the load that a particular belt can carry around certain sized gears at certain speeds given the number of other variables. These constants were deemed to be unprotectable since the relationships shown by the programs "are not invented or created; they already exist and are merely observed, discovered and recorded." Id. at 842-43.

h. Input/output formulas

(1) In Engineering Dynamics, Inc. v. Structural Software, Inc., 26 F.3d 1335, 1343-44, 1346 (1994), modified and reh'g denied, 46 F.3d 408 (5th Cir. 1995), the Fifth Circuit reversed a district court determination that input and output formulas in an applications program designed to solve structural engineering problems were unprotectable. The I/O formulas in that case consisted of a series of words and a framework of instructions that acted as a prompt for the insertion of relevant data.

(2) The precedential value of Engineering Dynamics, Inc. v. Structural Software, Inc. is uncertain. The Fifth Circuit relied heavily on Judge Robert Keeton's decisions in Lotus Development Corp. v. Paperback Software Int'l., 740 F. Supp. 37 (D. Mass. 1990) and Lotus Development Corp. v. Borland Int'l, Inc., 831 F. Supp. 223, 231 (D. Mass. 1993), rev'd, 49 F.3d 807 (1st Cir. 1995), aff'd mem., 516 U.S. 233 (1996) (4-4 decision), and in particular on Judge Keeton's finding (which was subsequently reversed by the First Circuit) that Lotus' menu command structure was entitled to copyright protection. The Fifth Circuit's holding that "the creativity inherent in [plaintiff's] program is proved by the existence of other, dissimilar structural engineering programs available in the market," is directly contradicted by the First Circuit's holding that creativity cannot transform a "method of operation" into protectable expression in Lotus Development Corp. v. Borland Int'l, Inc., 49 F.3d 807, 818 (1st Cir. 1995) ("the fact that there may be many different ways to operate a computer program, or even many different ways to operate a computer program using a set of hierarchically arranged command terms, does not make the actual method of operation chosen copyrightable . . ."), aff'd mem., 516 U.S. 233 (1996) (4-4 decision).

i. Threshold values. In Compaq Computer Corp. v. Procom Technology Inc., 908 F. Supp. 1409 (S.D. Tex. 1995), the court held that Compaq's threshold values (or the value of specific parameters selected by Compaq to trigger a prefailure warning in certain of Compaq's hard disk drives; when reached, Compaq would replace the drive if it was still under warranty) were protectable, although the order in which they appeared on a hard disk drive constituted unprotectable *scenes a faire*. In designing its prefailure warning system, Compaq determined both the number and particular parameters it would monitor *and* the appropriate

threshold value for each of the five parameters ultimately selected (which involved both engineering and business-related judgments).

2. Audiovisual works: screen displays and interfaces

   a. Screen displays may be protectable as audiovisual works even where the underlying code is not protectable as a literary work. Computer Associates Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 703 (2d Cir. 1992) (citing older cases).

   b. Interfaces protected as audiovisual works should be analyzed under the same test for evaluating protectability and infringement as software programs registered as literary works. Apple Computer, Inc. v. Microsoft Corp., 35 F.3d 1435, 1445 (9th Cir. 1994), cert. denied, 513 U.S. 1184 (1995).

3. What constitutes infringement?

   a. Elements. To prevail in an infringement action, a copyright owner generally must prove (1) ownership of a valid copyright, and (2) infringement by the defendant. E.g., Data East USA, Inc. v. Epyx, Inc., 862 F.2d 204, 206 (9th Cir. 1988). Since direct evidence of copying often is unavailable, a plaintiff may show infringement by evidence that (a) the defendant had access to plaintiff's work, and (b) the two works are substantially similar. E.g., Brown Bag Software v. Symantec Corp., 960 F.2d 1465 (9th Cir.), cert. denied, 506 U.S. 869 (1992). Where almost all of a work is comprised of elements licensed by the plaintiff or which are unprotectable, a plaintiff must show *virtual identicality*, rather than merely substantial similarity, in order to prevail in a copyright infringement action. See, e.g., Apple Computer, Inc. v. Microsoft Corp., 35 F.3d 1435, 1442 (9th Cir. 1994), cert. denied, 513 U.S. 1184 (1995).

   b. Ownership. A copyright registration certificate constitutes prima facie evidence of the validity of a copyright and the facts stated in the certificate, including the originality of the work and the ownership of the copyright. 17 U.S.C. § 410(c); Service & Training, Inc. v. Data General Corp., 963 F.2d 680, 688 (4th Cir. 1992). By presenting prima facie evidence of the validity of its claims, the burden of proof shifts to the defendant to dispute the validity of plaintiff's copyrights. E.g., Harris Market Research v. Marshall Marketing & Communications, Inc., 948 F.2d 1518, 1526 (10th Cir. 1991).

c. Infringement by literal code copying. Verbatim copying of object code or source code constitutes copyright infringement (assuming the portions of code copied include original, protectable elements). E.g., Computer Associates Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 702 (2d Cir. 1992); Kepner-Tregoe, Inc. v. Leadership Software, Inc., 12 F.3d 527, 534 (5th Cir.), cert. denied, 513 U.S. 820 (1994). Since the level of creativity required for copyright protection is low (supra § I(C)(1)), direct evidence that a defendant copied substantial portions of a program generally will be sufficient to show copyright infringement.

d. Infringement by non-literal copying/"look and feel" infringement Most of the battles over the scope of copyright protection for computer software have been fought in non-literal infringement cases, where the plaintiff alleges that the "look and feel" of a program (but not necessarily the literal code) have been copied.

(1) Third Circuit:

(a) The Third Circuit was the first to define the scope of copyright protection in cases of alleged non-literal infringement. In Whelan Associates, Inc. v. Jaslow Dental Laboratory, Inc., 797 F.2d 1222 (3d Cir. 1986), cert. denied, 479 U.S. 1031 (1987), the Third Circuit adopted a broad view of the scope of copyright protection for computer software, holding that copyright protection extends beyond a program's literal code to its "structure, sequence and organization." Under the Third Circuit's test, as a practical matter, the "idea" of a program is defined very narrowly, and everything not necessary to the program's purpose or function is deemed to constitute protectable expression. 797 F.2d at 1236.

(b) Especially since the U.S. Supreme Court's rejection of the "sweat of the brow" doctrine in Feist Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340, 361 (1991), the Third Circuit test has been severely criticized as taking an unduly broad view of the scope of copyright protection. E.g., Computer Associates Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 706 (2d Cir. 1992); Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510, 1525 (9th Cir. 1992); CMAX/Cleveland, Inc. v. UCR, Inc., 804 F. Supp. 337, 352 (M.D. Ga. 1992); Micro Consulting, Inc. v. Zubeldia, 813 F. Supp. 1514,

1528 (W.D. Ok. 1990), aff'd mem., 959 F.2d 245 (10th Cir. 1992). Whelan Associates, however, has not been modified or overruled by the Third Circuit.

(2) Second, Third, Fifth, Ninth, Tenth and Eleventh Circuits:

(a) Most circuits, including even the Third Circuit, now apply Abstraction - Filtration - Comparison. E.g., Computer Associates Int'l, Inc. v. Altai, Inc., 982 F.2d 693 (2d Cir. 1992); Dun & Bradstreet Software Services v. Grace Consulting, Inc., 307 F.3d 197, 214, 217 (3d Cir. 2002); Engineering Dynamics, Inc. v. Structural Software, Inc., 26 F.3d 1335 (1994), modified and reh'g denied, 46 F.3d 408 (5th Cir. 1995); Brown Bag Software v. Symantec Corp., 960 F.2d 1465, 1472 (9th Cir.), cert. denied, 506 U.S. 869 (1992); Gates Rubber Co. v. Bando Chemical Industries, Ltd., 9 F.3d 823 (10th Cir. 1993); Bateman v. Mnemonics, Inc., 79 F.3d 1532 (11th Cir. 1996); see also, e.g., Control Data Systems, Inc. v. Infoware, Inc., 903 F. Supp. 1316 (D. Minn. 1995) (applying abstraction - filtration - comparison).

(b) Under the Altai Abstraction – Filtration - Comparison test, courts must first dissect the structure of the copyright owner's program to isolate each level of abstraction, beginning with protectable expression (typically object code) and ending with the unprotectable idea of the program (its ultimate function). The Second Circuit describe this first part of the test, known as "abstraction," as resembling "reverse engineering on a theoretical plane." Courts next must examine each component part of the program (at each level of abstraction) to filter out unprotectable aspects of the program, including expression not original to the author, aspects which constitute "the idea" of the program, expression necessarily incident to the idea, expression in the public domain and expression dictated by external factors (like the mechanical specifications of the hardware on which the program was designed to run, the need to make the program compatible with other programs and the demands of the industry served by the program). Finally, a court will be "left with a kernel, or possibly kernels, of creative expression" which

would then be compared with the allegedly infringing program to determine whether protectable elements of the copyright owner's program have been infringed.

(3) First Circuit: the First Circuit declined to apply the majority Altai test in Lotus Development Corp. v. Borland Int'l, Inc., 49 F.3d 807 (1st Cir. 1995), aff'd mem., 516 U.S.. 233 (1996) (4-4 decision), holding that the application of the test in that case could actually be misleading. The First Circuit wrote that, in instructing courts to abstract the various levels of a software program, the test implicitly assumed that there was a base level for each program that included copyrightable subject matter.

e. Infringement based on exceeding the scope of a license/ "virtual identicality" required in some instances. In a true license, a licensor grants a licensee fewer rights than it is granted under patent or copyright law. A licensee who exceeds the scope of its license may be held liable for copyright infringement. E.g., S.O.S., Inc. v. Payday, Inc., 886 F.2d 1081, 1087-89 (9th Cir. 1989).

f. Infringement through unauthorized importation. A plaintiff may establish infringement by evidence that, without the copyright owner's authorization, the defendant imported and then sold in the United States goods protected by a U.S. copyright. 17 U.S.C. § 602(a); BMG Music v. Perez, 952 F.2d 318, 319-20 (9th Cir. 1992), cert. denied, 505 U.S. 1206 (1992).

D. Liability Under the Computer Software Rental Amendments Act

1. The Computer Software Rental Amendments Act prohibits any person "for the purposes of direct or indirect commercial advantage [to] dispose of, or authorize the disposal of . . ." a computer program acquired on or after 12/1/90 "by rental, lease or lending, or by any other act or practice in the nature of rental, lease or lending." 17 U.S.C. § 109(b)(1)(A). As illustrated in the following case, courts will look behind a defendant's characterization of a transaction to evaluate if the Act has been violated.

2. Central Point Software, Inc. v. Global Software & Accessories, Inc., 880 F. Supp. 957 (E.D.N.Y. 1995).

a. Deferred billing. Judge Leonard Wexler of the Eastern District of New York held that a computer software company's "sale" of software under a deferred billing plan amounted to the rental of software prohibited by the Act. Under the plan, customers paid a small "nonrefundable deposit" for the software and were not billed

for the balance if they returned it within five days. Judge Wexler found that the transactions were tantamount to rentals, since (a) defendant's brochures advertised the "nonrefundable deposit," not the purchase price of software, (b) nearly 100% of the software was returned, (c) the deposits were comparable to rental fees, (d) the short term of the agreements was comparable to a rental term, obviously allowing the defendant to use the same copy of software in other transactions, and (e) the customer was not given the software manufacturer's registration card unless the full purchase price was paid.

b. Software upgrades. Judge Wexler also held the defendant liable for renting customers post-December 1, 1990 upgrades of programs it acquired before December 1, 1990. Judge Wexler held that the company's right to lawfully rent software acquired before December 1, 1990 did not extend to later upgrades of the same programs.

E. The Fair Use Defense

1. Multi-part balancing test. Fair use is a complete defense to copyright infringement. 17 U.S.C. § 107. The defense applies where a work is used "for purposes such as criticism, comment, news reporting, teaching . . . scholarship or research . . . ." Id. In evaluating whether the fair use defense is available, courts must evaluate (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work. Id.

2. Reverse engineering of software

a. Disassembly of object code was held to be a fair use in Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992) because (a) disassembly was necessary to analyze those aspects of the program which were unprotectable, and (b) Accolade had a legitimate interest in analyzing those aspects of the program (to determine how to make its cartridges compatible with the Genesis console); see also Sony Computer Entertainment, Inc. v. Connectix Corp., 203 F.3d 596, 607 (9th Cir. 2000).

b. Disassembly was held not to be a fair use in Atari Games Corp. v. Nintendo of America Inc., 975 F.2d 832, 834 (Fed. Cir. 1992) because Atari did not own an authorized copy of the plaintiff's program, which is a precondition for invoking the fair use defense. In dicta, the court wrote that intermediate copying is fair use when

the nature of the work makes such copying necessary to understand the ideas and processes inherent in the program. Reverse engineering object code to discern the unprotectable ideas therefore may be fair use, the Federal Circuit wrote, provided that the reproduction is limited in scope and does not involve commercial exploitation of the protected aspects of the work.

c. For a more extensive discussion of reverse engineering as fair use, see William S. Coats & Heather D. Rafter, "The Games People Play: *Sega v. Accolade* and the Right to Reverse Engineer Software," 15 Hastings Communications & Entertainment L.J. 557 (1993).

3. Parody. Parody is not, *per se*, fair use. In order to constitute a fair use parody, a work generally must be targeted at the original work and not merely borrow its style. See Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569 (1994) (sampling of a copyrighted song may be fair use when used in a new parody work); see also SunTrust Bank v. Houghton Mifflin Co., 268 F.3d 1257 (11th Cir. 2001) (reversing the lower court's entry of a preliminary injunction upon finding that the defendant's book, "The Wind Done Gone," constituted a fair use parody of "Gone With the Wind.").

4. Taping television transmissions for future viewing. The practice of recording television broadcasts on videocassette recorders is a fair use when the copying is undertaken for private, non-commercial purposes. Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984). The decision was supported by evidence that this form of copying represented "time shifting," or the practice by viewers of recording television transmissions to watch at more convenient times.

5. "File Sharing" Downloadable Music Files

a. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

Napster created and released software that allowed third parties to make music files on their hard drives available to others in cyberspace who were using Napster's service, thereby facilitating large-scale copyright infringement. The Ninth Circuit rejected Napster's fair use defense.

(1) Purpose and character of the use. The Ninth Circuit found that the purpose and character of the work – the first of the four fair use factors set forth in the Copyright Act – weighed against Napster because its use was not transformative, but merely involved the retransmission of an original work in a new medium.

(2) Commercial use. The Ninth Circuit found use of the Napster service to be commercial because, in the words of the district court, (1) "a host user sending a file cannot be said to engage in a personal use when distributing that file to an anonymous requester" and (2) "Napster users get for free something they would ordinarily have to buy." In so ruling, the appellate panel emphasized that "[d]irect economic benefit is not required to demonstrate a commercial use. Rather, repeated and exploitative copying of copyrighted works, even if the copies are not offered for sale, may constitute a commercial use." In addition, the court noted that the definition of a financially motivated transaction for purposes of criminal copyright infringement includes trading infringing copies of a work for other items, such as other protected works.

(3) Nature of the use. The panel concluded that the nature of the use weighed against a finding of fair use because musical compositions and sound recordings are creative in nature. Similarly, the portion used weighed against a finding of fair use because full length versions of protected songs were copied.

(4) Effect on the market. The court concluded that the effect on the market weighed against a finding of fair use because Napster both (1) reduced audio CD sales among college students (who, with their access to high speed networks, were primary users of Napster's service) and (2) retarded the development of legitimate online music distribution services by raising barriers to plaintiffs' own entry into the market for digital downloading of music. In so ruling, the appellate court cited with approval the unreported district court opinion in L.A. Times v. Free Republic, 54 U.S.P.Q.2d 1453 (C.D. Cal. 2000), for the proposition that the lack of harm to an established market cannot deprive the copyright owner of the right to develop alternative markets for its works.

(5) Sampling. The court dismissed the contention that the distribution of samples – or excerpts of full songs – might promote the sales of genuine copies, thereby making the practice less commercial, inasmuch as both the market for CD sales and online distribution were harmed by Napster. The Ninth Circuit also noted that authorized samples generated royalties for the record company plaintiffs and that free promotional downloads were highly regulated.

(6) Space shifting. Napster's space shifting argument – or the defense that some users downloaded copies of songs that they already owned – was rejected because in the cases relied upon by Napster – RIAA v. Diamond Multimedia Systems, Inc., 180 F.3d 1072 (9th Cir. 1999) and Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984) – the methods of space or time shifting "did not also simultaneously involve distribution of the copyrighted material to the general public . . . only to the original user."

b. In UMG Recordings, Inc. v. MP3.com, Inc., 92 F. Supp. 2d 349 (S.D.N.Y. 2000), the court entered partial summary judgment in favor of the plaintiffs, ruling that MP3's practice of copying music files to a database to facilitate user copying (in connection with its my.mp3.com service) constituted a violation of the Copyright Act. MP3 had taken a number of precautions designed to ensure that only owners of legitimate copies of protected CR ROMs could make copies of the music files stored on its database. Among other things, it required users to certify that they owned a genuine copy, insert a genuine copy in their computer disk drive or purchase a copy from a cooperating online retainer. MP3 had argued that this practice allowed users to make personal copies of songs permitted under Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984). The court, however, found that by making thousands of songs available online for a commercial purpose, MP3.com's acts of copying (as opposed to end user copying) were not a fair use. The case ultimately settled with MP3.com agreeing to pay royalties to certain settling record companies.

6. Photocopying articles for convenience. American Geophysical Union v. Texaco, Inc., 37 F.3d 881 (2d Cir. 1994), pet. for cert. filed (Apr. 24, 1995); American Geophysical Union v. Texaco, Inc., 60 F.3d 913 (2d Cir. 1995).

a. 1994 opinion. The Second Circuit held that a scientist's practice of photocopying individual scientific articles that he kept in personal files in his office as a matter of convenience (to save the time it otherwise would have taken to retrieve the articles in journals maintained in Texaco's library) did not constitute fair use in view of the predominantly archival (rather than research-oriented) purpose of the copying, and because of the harm this practice caused to the publisher's market for licensing photocopying. The majority analyzed the scientist's copying as an "intermediate use," as that term was used in Sega Enterprises Ltd. v. Accolade, Inc., supra, because Texaco's photocopying "served, at most, to facilitate [the scientist's] research, which in turn might have led to the development of new products and technology that could have

improved Texaco's commercial performance." 37 F.3d at 889. Unlike in Sega Enterprises, the Second Circuit did not find the fair use defense applicable.

b. Amended opinion. The Second Circuit took the unusual step of amending its opinion in July 1995, after Texaco had asked the Circuit to defer ruling on its petition for rehearing en banc based on the parties' agreement in principle to settle the case. In his amended opinion, Judge Newman emphasized that the decision rested on a finding of "institutional, systematic copying." 60 F.3d at 931. He wrote that "[w]e do not deal with the question of copying by an individual for personal use in research or otherwise (not for resale), recognizing that under the fair use doctrine or the de minimis doctrine, such a practice by an individual might well not constitute an infringement." Id. at 916; D. Pines, "Aim to Narrow Circuit Ruling on 'Fair Use'; Amended Decision Issued in Controversial Case," N.Y.L.J., July 19, 1995, at 1. Although the Second Circuit purports to distinguish between individual and institutional copying, this distinction is not clearly apparent from the facts of the Texaco case itself, making further litigation likely.

c. Law lags behind technology. The Texaco opinion also provides an example of how changes in the law lag behind technological innovations. In Texaco, the Second Circuit lamented congressional inaction, writing that, "[a]s with the development of other easy and accessible means of mechanical reproduction of documents, the invention and widespread availability of photocopying technology threatens to disrupt the delicate balances established by the Copyright Act." 37 F.3d at 885-86.

d. Implications online. The problem of technology facilitating copyright infringement is even more acute online, where, for example, information (in the form of sound, video, images and/or written text) accessible in digital form may be attached to an email message and posted to a website or transmitted in a matter of seconds to hundreds, or even thousands of people. While widespread dissemination of protected material would constitute infringement, the parameters of "fair use" in cyberspace are still developing. See Ian C. Ballon, "Determining Fair Use in Cyberspace," L.A. Daily Journal, Sept. 6, 1995, at 7.

7. The retransmission over the Internet of infringing material (the Church of Scientology cases). The extent to which protected text may be posted online for the purpose of criticism was litigated in three lawsuits involving former members of the Church of Scientology (and in a fourth suit involving a nonmember) who posted confidential Scientology documents (that the church contends constitute trade secrets) online, ostensibly to

embarrass and criticize the church and expose Scientology teachings. In all three suits against former Church members, the defendants included both the individuals who posted the protected works and their Internet access providers.

a. In Religious Technology Center v. F.A.C.T.Net, Inc., 901 F. Supp. 1519 (D. Colo. 1995), Judge Kane denied plaintiff's motion for a preliminary injunction finding defendant's posting of unpublished Scientology documents a fair use "to advance understanding of issues concerning the Church which are the subject of ongoing public controversy," in part because there was no "potential for financial loss to the church."

b. Netcom litigation — the individually named defendant. In a much more thorough analysis, Judge Whyte of the Northern District of California rejected defendant Erlich's fair use defense in Religious Technology Center v. Netcom On-Line Communication Services, Inc., 923 F. Supp. 1231 (N.D. Cal. 1995), finding the defense inapplicable because of the high percentage of plaintiffs' works copied, the extent of verbatim copying and the minimal amount of added criticism or commentary. Judge Whyte also ruled that the scope of permissible fair use was narrower in this case because plaintiff's works were unpublished. Otherwise, the informational (as opposed to creative) nature of the works would have allowed for a broader interpretation of fair use. 923 F. Supp. at 1246. Defendant Erlich's argument that a preliminary injunction would operate as a prior restraint on his First Amendment rights was rejected on the grounds that the fair use defense incorporated in the 1976 Copyright Act "embodies a balance between the rights of copyright holders, guaranteed by the Constitution, U.S. Const. art. I, § 8, and the protections of the First Amendment." 923 F. Supp. at 1258 (citations omitted).

c. Netcom litigation — the internet access provider. In a later opinion on November 21, 1995, Judge Whyte ruled that there was a genuine question of fact as to whether Netcom, the Internet access provider for the BBS where Erlich posted his infringing messages, had a valid fair use defense. The court denied Netcom's motion for summary judgment in light of evidence that it knew that Erlich's use was infringing and had the ability to prevent further distribution. In analyzing the first fair use factor, the purpose and character of the use, the court concluded that Netcom's "use" of plaintiffs' works was to carry out its commercial function as an Internet access provider, writing that "Netcom's use, though commercial, also benefits the public in allowing for the functioning of the Internet and the dissemination of other creative works, a goal of the Copyright Act." 907 F. Supp. at 1379 (citations

omitted). The court also noted that, although Netcom gained financially from its distribution of messages over the Internet, its financial incentive was unrelated to the infringing activity and Netcom received no direct financial benefit from Erlich's acts of infringement. The court determined that the second factor, the nature of the copyrighted work, was not important to its fair use analysis because "Netcom's use of the works was merely to facilitate their posting to the Usenet, which is an entirely different purpose than plaintiffs' use (or, for that matter, Erlich's use) . . . ." Id. at 1379 (citations omitted). In analyzing the third factor, the amount and substantiality of the portions used, the court deemed immaterial the extent of Netcom's copying (despite the fact that it was substantial) because Netcom made available to the Usenet exactly what was posted by Erlich; "Netcom copied no more of plaintiffs' works than necessary to function as a Usenet server. Like the defendant in Sega v. Accolade, Netcom had no practical alternative way to carry out its socially useful purpose; a Usenet server must copy all files, since the prescreening of postings for potential copyright infringement is not feasible." Id. at 1380, citing Sega Enterprises, Ltd. v. Accolade, Inc., 977 F.2d 1510, 1526-27 (9th Cir. 1992). Finally, the court found that there was a genuine issue of fact with respect to the fourth factor, the effect of the use upon the potential market for the work, which the court deemed to be the most significant factor. 907 F. Supp. at 1380.

d. Lerma – initial orders. In Religious Technology Center v. Lerma, 897 F. Supp. 260 (E.D. Va. 1995), the court entered a temporary restraining order against Arnaldo Lerma, a former Scientology member, and Digital Gateway Systems, Lerma's Internet access provider. Thereafter, Lerma gave copies of the documents posted online to a Washington Post reporter who quoted small excerpts in a news article about the lawsuit. The reporter, Marc Fisher, and the Washington Post subsequently were added as defendants to the lawsuit. On August 30, 1995, the court denied plaintiff's motion for a temporary restraining order and preliminary injunction against Fisher and the Washington Post on fair use grounds in large measure because the Washington Post was able to acquire the same documents quoted in the news article by photocopying court records in another lawsuit pending in California, during a brief period of time when the court records in that case were not under seal. In a later opinion, on November 28, 1995, the court granted summary judgment in favor of Fisher and the Washington Post. Religious Technology Center v. Lerma, 908 F. Supp. 1362 (E.D. Va. 1995). However, Judge Brinkema ordered the Washington Post defendants to refrain from making additional copies of the documents or filing them with the court except under seal. In

focusing its fair use analysis on the small excerpts of plaintiff's works reproduced in the Washington Post article, the court apparently overlooked the issue of whether the Washington Post's wholesale photocopying of protected works from a court file constituted copyright infringement. See American Geophysical Union v. Texaco, Inc., 60 F.3d 913 (2d Cir. 1995); supra § I(E)(6).

e. Lerma — First Amendment arguments. In still another ruling in Religious Technology Center v. Lerma, 908 F. Supp. 1353 (E.D. Va. 1995), the court on November 29, 1995 denied plaintiffs' motion for a preliminary injunction against defendants Lerma and Digital Gateway Systems and denied plaintiffs' "Emergency Motion for Reconsideration" of the court's August 30, 1995 order denying injunctive relief against the Washington Post defendants. In so ruling, Judge Brinkema rejected plaintiffs' argument that they were being denied their right to free exercise of their religion because, according to the Scientology religion, the texts at issue had to be kept confidential (except from a select few who had achieved certain spiritual levels). Plaintiffs had argued that dissemination of their confidential materials would decimate the scientology religion, and therefore was comparable to "compelling a Protestant to dispute the Resurrection, ordering a fundamentalist to read the Bible [non-literally], compelling an observant Jew to eat pork, or compelling an observant Catholic to have an abortion." Judge Brinkema, however, rejected these analogies, and wrote that, "[i]n their effort to enjoin the Post, the RTC is essentially urging that we permit their religious belief in the secrecy of the AT documents to 'trump' significant conflicting constitutional rights. In particular, they ask us to dismiss the equally valid First Amendment protections of freedom of the press." Stated differently, the court characterized plaintiffs' argument as a request to "allow the Free Exercise Clause to deflate the doctrine of fair use as embodied in the copyright statute . . . ." In the alternative, the court ruled that plaintiffs were barred from injunctive relief by the unclean hands doctrine because their zealous prosecution of this lawsuit and the related F.A.C.T.Net case were really intended to stifle legitimate criticism of the Church, rather than merely protect confidential works.

8. Web browsing. When a user browses through pages on the worldwide web (or elsewhere) screen displays are automatically downloaded to cache or screen memory. In Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995), Judge Whyte wrote in dicta that browsing could cause an infringing copy to be made in screen memory, but that such copying would be deemed to be fair use because "the temporary copying involved in browsing is only

necessary because humans cannot otherwise perceive digital information." Id. at 1378 n.25. Judge Whyte characterized digital browsing as "the functional equivalent of reading, which does not implicate the copyright laws and may be done by anyone in a library without the permission of the copyright owner." Id.; see infra § I(F)(7)(e).

9. Shareware. In Storm Impact, Inc. v. Software of the Month Club, 13 F. Supp. 2d 782 (N.D. Ill. 1998), the court ruled that the defendant's practice of aggregating (free) shareware software from the Internet, which it sold as part of CD ROM compilations, constituted copyright infringement in violation of the terms of the plaintiff's shareware license. Storm Impact is a reminder that material may not necessarily be freely copied merely because it is accessible without charge online.

10. Copying by visual search engines. In Kelly v. Arriba Software Corp., 336 F.3d 811 (9th Cir. 2003), the Ninth Circuit ruled that the practice of a visual search engine – in making unauthorized thumbnail copies of photographs located on sites responsive to user search requests – constituted a fair use under copyright law. The images in that case were generated indiscriminately based on user requests and served a functional, rather than creative purpose (to facilitate searching and indexing practices). In an earlier decision vacated by this ruling, Kelly v. Arriba Software Corp., 280 F.3d 934 (9th Cir. 2002), the Ninth Circuit had further ruled that the defendant's earlier practice of making available via in-line links and frames full-size copies of the photographs as they had appeared on indexed sites (but with the surrounding text and other web content removed) violated the copyright owner's public display right and did not constitute a fair use.

F. The Third-Party Liability of Online Content and Access Providers

1. Direct Liability

a. Strict liability. Under the 1976 Copyright Act, liability for direct infringement may be imposed regardless of a defendant's intent. Although a party's innocence may color the way a case is decided, culpability technically is only relevant in determining the amount of an award of statutory damages (which may be reduced to as little as $200 in cases of innocent infringement; see 17 U.S.C. § 504(c)) or in limited circumstances where a work first published prior to March 1, 1989, did not contain a copyright notice. See id. § 405(b). As a practical matter, this means that a defendant's alleged innocence rarely will be a significant legal issue in a direct infringement case involving more recent works since a copyright plaintiff has sole discretion whether to elect statutory damages in lieu of actual damages (and intent is not considered in assessing actual damages). See id. § 504(c). A defendant's bad faith, on the

other hand, may be relevant in negating a defense of fair use. See Religious Technology Center v. Netcom On-Line Communication Services, Inc., 923 F. Supp. 1231, 1244 (N.D. Cal. 1995).

b. Volitional conduct or causation required. Even though the Copyright Act imposes strict liability, courts have held that some element of direct action or volitional conduct is required before a service provider may be held directly liable because infringing content has been posted on its service. See Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361, 1370 (N.D. Cal. 1995) (Usenet postings; in order to find direct liability, "there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party."); see also CoStar Group, Inc. v. Loopnet, Inc., 373 F.3d 544 (4th Cir. 2004) (following Netcom); Sega Enterprises Ltd. v. MAPHIA, 948 F. Supp. 923, 932 (N.D. Cal. 1996) (no evidence that the BBS operator caused infringing copies to be made merely by operating a BBS where third parties posted infringing software); Marobie-FL, Inc. v. National Association of Fire Equipment Distributors, 983 F. Supp. 1167 (N.D. Ill. 1997) (company which hosted a website on which infringing material was posted held not liable for direct infringement because, even though it "provide[d] a service somewhat broader than the . . . . Internet access provider in Religious Technology Center . . . [it] only provided the means to copy, distribute or display plaintiff's works, much like the owner of a public copy machine used by a third party to copy protected material."); Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503 (N.D. Ohio 1997) ("some element of direct action" is required). But see Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993) (holding a BBS operator liable for infringing photographs potentially posted by a third party because the Copyright Act imposes strict liability).

2. Contributory infringement.

a. Culpable conduct required. "'[O]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another,' may be held liable as a contributory infringer." Sega Enterprises Ltd. v. MAPHIA, 857 F. Supp. 679, 686 (N.D. Cal. 1994); see generally Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 435 (1984) ("The absence of . . . express language in the copyright statute does not preclude the imposition of liability for copyright infringements on certain parties who have not themselves engaged in the infringing activity for vicarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of

the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another").

b. Liability for contributory infringement generally requires a showing of (1) direct infringement by a third party; (2) actual or constructive knowledge by the defendant; and (3) substantial participation by the defendant in the infringing activities. UMG Recordings, Inc. v. Bertelsmann, 222 F.R.D. 408 (N.D. Cal. 2004).

c. The Ninth Circuit in MGM Studios, Inc. v. Grokster Ltd., 380 F.3d 1154 (9th Cir. 2004) modified the traditional test, at least in cases involving peer-to-peer networks, by requiring that actual, not constructive knowledge, must be shown, in cases where the product at issue is capable of "substantial" or "commercially significant" noninfringing uses (based on either current or potential future use). This ruling is controversial and may not be followed in other circuits. See Ian C. Ballon, "Ninth Circuit's *Grokster* Decision Changes the Law of Secondary Copyright Liability," *California Copyright Conference Newsletter*, Sept. 2004. The *Grokster* case presently is before the U.S. Supreme Court.

3. Vicarious liability. Vicarious liability may be imposed where the defendant (1) has the right and ability to supervise the infringing activity, and (2) has a direct financial interest in such activities. E.g., Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996). By definition, vicarious liability, like direct liability, may be imposed without regard to a defendant's intent. Whether and to what extent a service provider may actually be able to supervise or control the infringing conduct of its users is an open question for many services, including NSPs, and legitimate ISPs that merely provide access to consumers.

a. Individual and investor liability. The vicarious liability doctrine may be used to hold the individual owners of corporate sites and services (or other limited liability entities), or even venture capital or other investors, personally liable in circumstances where state law otherwise would not allow a plaintiff to pierce the corporate veil. See, e.g., Playboy Enterprises, Inc. v. Webbworld, Inc, 999 F. Supp. 573 (N.D. Tex. 1997) (LLC owners), aff'd mem, 168 F.3d 486 (5th Cir. 1998); infra § I(F)(8); UMG Recordings, Inc. v. Bertelsmann, 222 F.R.D. 408 (N.D. Cal. 2003) (denying motions to dismiss by Bertelsmann and Hummer Winblad Venture Partnerships based on specific allegations that these investors assumed control of Napster and directed its operations). But see Perfect 10, Inc. v. VISA Int'l Service Ass'n, Case No. C 04 0371 JW (N.D. Cal. Aug. 5, 2004) (dismissing claims for contributory and vicarious infringement asserted against credit card companies

based on the allegedly infringing conduct of various website vendors who used these companies to process payments).

b. Even an Internet service that does not charge money may be found to have a "financial interest" in underlying acts of infringement. See A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); infra § I(F)(9).

c. In MGM Studios, Inc. v. Grokster Ltd., 380 F.3d 1154 (9th Cir. 2004), the Ninth Circuit held that various P2P networks could not be held vicariously liable because they did not have the ability to control user conduct at the moment in time when files were transferred by users. This ruling is controversial. See Ian C. Ballon, "Ninth Circuit's *Grokster* Decision Changes the Law of Secondary Copyright Liability," *California Copyright Conference Newsletter*, Sept. 2004. The case presenly is before the U.S. Supreme Court.

4. Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993).

a. Facts: Defendant George Frena operated a subscription computer bulletin board service (BBS). For a fee, subscribers could log onto Frena's BBS and upload and download digitized copies of photographs. Frena argued that he allowed subscribers to upload whatever they wanted onto the BBS. At least 170 images available in Frena's BBS were taken from 50 of Playboy's copyrighted magazines. Frena's name, BBS name and telephone number appeared on each of the infringing images.

b. Holding: The trial court granted partial summary judgment for the plaintiff, holding that Frena had violated Playboy's exclusive rights as a copyright owner to distribute and display its photographs. Id. at 1556-57. The court rejected Frena's argument that he was unaware of the infringement since intent or knowledge is only relevant to the issue of statutory damages, not liability for copyright infringement. Id. at 1559.

5. Sega Enterprises Ltd. v. MAPHIA, 857 F. Supp. 679 (N.D. Cal. 1994).

a. Facts: Defendants operated a computer bulletin board called "MAPHIA" on which unauthorized copies of plaintiff's copyrighted videogames were uploaded and downloaded by bulletin board subscribers. Defendants actively encouraged subscribers to upload and download bootlegged copies of Sega's videogames and even marketed hardware and software that could be used to make unauthorized copies of Sega videogames, which

in genuine form are stored on a cartridge in a read-only memory (ROM) chip.

b. Holding: preliminary injunction granted. Defendants were held liable for copyright infringement as contributory infringers based on their "provision of facilities, direction, knowledge and encouragement . . . ." Id. at 686-87.

6. Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).

a. Procedural Background: In February 1995, the Church of Scientology brought suit in federal court in San Jose against Dennis Erlich, a former Scientology minister who allegedly posted copyrighted material authored by L. Ron Hubbard on a Usenet group named "alt.religion.scientology"; Netcom On-Line Communication Services, an Internet access provider; and Tom Klemesrud, the operator of the BBS where Erlich posted his material (which was connected to the Internet via Netcom). Plaintiffs allege that Erlich stole their trade secrets, that Erlich's postings infringe plaintiffs' copyrights and that Netcom and Klemesrud are also liable for Erlich's alleged copyright infringement and misappropriation of trade secrets. A preliminary injunction issued against Erlich remains in effect. See Religious Technology Center v. Netcom On-Line Communication Services, Inc., 923 F. Supp. 1231 (N.D. Cal. 1995); supra § I(E)(7)(b).

b. November 1995 opinion: On November 21, 1995, Judge Whyte denied Netcom's motion for summary judgment and Klemesrud's motion for judgment on the pleadings because he found a triable issue of fact on plaintiffs' claim for contributory infringement. Judge Whyte found no evidence to support claims of direct infringement against Netcom or Klemesrud or vicarious liability against Netcom, although he granted plaintiffs thirty days' leave to amend their complaint to state a claim for vicarious liability against defendant Klemesrud, if they could do so in good faith. Judge Whyte also denied plaintiffs' application for a preliminary injunction against Netcom and Klemesrud.

c. Facts relevant to the motions: After failing to convince defendant Erlich to stop posting scientology documents on the "alt.religion.scientology" Usenet group, plaintiffs contacted defendants Klemesrud and Netcom demanding that they take action to stop Erlich's postings. Klemesrud responded by asking for proof that plaintiff owned copyrights to the works posted by Erlich; plaintiffs refused Klemesrud's request as unreasonable. Netcom took no action after it was notified by plaintiffs, claiming

that it could not block Erlich's postings without shutting out all of the users of Klemesrud's BBS. Unlike on-line services that provide content, such as CompuServe, America Online, or Prodigy, Netcom, as merely an Internet access provider, does not create or control the content of the information available to its subscribers.

The parties did not dispute the basic processes that occurred when Erlich posted his allegedly infringing messages to the "alt.religion.scientology" newsgroup:

> Erlich connects to Klemesrud's BBS using a telephone and a modem. Erlich then transmits his messages to Klemesrud's computer, where they are automatically briefly stored. According to a prearranged pattern established by Netcom's software, Erlich's initial act of posting a message to the Usenet results in the automatic copying of Erlich's message from Klemesrud's computer onto Netcom's computer and on to other computers on the Usenet. In order to ease transmission and for the convenience of Usenet users, Usenet servers maintain postings from newsgroups for a short period of time — eleven days for Netcom's system and three days for Klemesrud's system. Once on Netcom's computers, messages are available to Netcom's customers and Usenet neighbors, who may then download the messages to their own computers. Netcom's local server makes available its postings to a group of Usenet servers, which do the same for other servers until all Usenet sites worldwide have obtained access to the postings, which takes a matter of hours.

907 F. Supp. at 1367-68.

d. Erlich's transmissions held to create "copies" on Klemesrud's BBS and Netcom's computers. The court, applying MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993), cert. dismissed, 510 U.S. 1033 (1994) (supra § I(A)(2)(b)(1)), held that Erlich's act of sending a message to the "alt.religion.scientology" Usenet group caused "copies" of plaintiffs' works to be created on both Klemesrud's and Netcom's storage devices (even though the messages remained on their systems for at most 11 days).

e. Netcom not liable for direct infringement. The court held that Netcom could not be held liable for direct infringement, even though the Copyright Act is a strict liability statute, because "there should still be some element of volition or causation which is

lacking where a defendant's system is merely used to create a copy by a third party." 907 F. Supp. at 1370.

(1) MAI Distinguished. Judge Whyte wrote that "Netcom's actions, to the extent that they created a copy of plaintiffs' works, were necessary to having a working system for transmitting Usenet postings to and from the Internet. Unlike the defendant in MAI, neither Netcom nor Klemesrud initiated the copying. . . . Netcom's and Klemesrud's systems can operate without any human intervention. Thus, unlike MAI, the mere fact that Netcom's system incidentally makes temporary copies of plaintiffs' works does not mean Netcom has caused the copying." Id. at 1368-69.

(2) Ruling Contradicts NII White Paper. Disagreeing with the recommendations of the NII White Paper that BBS operators be held strictly liable, Judge Whyte concluded that "[t]he court does not find workable a theory of infringement that would hold the entire Internet liable for activities that cannot reasonably be deterred. Billions of bits of data flow through the Internet and are necessarily stored on servers throughout the network and it is thus practically impossible to screen out infringing bits from noninfringing bits. Because the court cannot see any meaningful distinction (without regard to knowledge) between what Netcom did and what every other Usenet server does, the court finds that Netcom cannot be held liable for direct infringement." Id. at 1372-73.

f. Netcom's potential liability for contributory infringement. The court held that a triable issue of fact existed as to whether Netcom could be held liable for contributory infringement, which the court wrote is imposed "where the defendant, 'with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another.'" 907 F. Supp. at 1373, quoting Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971). The court found that it was undisputed that Netcom initially did not know that Erlich was infringing, but there was a question of fact about whether Netcom knew or should have known that Erlich had infringed plaintiffs' copyrights after it received notice from plaintiffs and failed to investigate. Although a mere unsupported allegation of infringement may not automatically put a defendant on notice of infringing activity,

where works contain copyright notices within them, as here, it is difficult to argue that a defendant did not know that the works were copyrighted. To require proof of valid registrations would be impractical and would perhaps take too long to verify . . . the court is more persuaded by the argument that it is beyond the ability of a BBS operator to quickly and fairly determine when a use is not infringement where there is at least a colorable claim of fair use. Where a BBS operator cannot reasonably verify a claim of infringement, either because of a possible fair use defense, the lack of copyright notices on the copies, or the copyright holder's failure to provide the necessary documentation to show that there is a likely infringement, the operator's lack of knowledge will be found reasonable and there will be no liability for contributory infringement for allowing the continued distribution of the works on its system.

Id. at 1374.

g. Netcom not liable for vicarious infringement. The court held that plaintiffs failed to show a triable issue of fact on the issue of whether Netcom received a direct financial benefit from Erlich's infringement, precluding plaintiffs' claim for vicarious liability. The court wrote that to prove vicarious liability, a plaintiff must show the defendant (1) had the right and ability to control the infringer's acts and (2) received a direct financial benefit from the infringement. 907 F. Supp. at 1375, citing Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 306 (2d Cir. 1963). The court also reiterated that unlike contributory infringement, knowledge need not be shown.

(1) Right and ability to control. The court found conflicting evidence on the issue of whether Netcom had the ability to control Erlich's infringing conduct. As merely an access provider, Netcom does not create or control the content of the information available to its subscribers, and it does not monitor messages as they are posted. Netcom claimed that it could not limit Erlich's access to the Usenet without "kicking off all 500 subscribers of Klemesrud's BBS." However, Netcom had, in the past, suspended the accounts of subscribers who have violated its terms and conditions (for example, when individuals had commercial software in their posted files). In addition, Netcom admitted during the litigation that (while not currently configured to do so) it might have been possible to reprogram its system to screen postings containing particular words or coming from particular individuals. 907 F. Supp. at 1375-76.

(2) Direct financial benefit. The court found that plaintiffs were unable to show that Netcom received a direct financial benefit from the infringing activities of its users. Netcom receives a fixed fee and no evidence was presented that the infringement by Erlich, or any other user of Netcom's services, in any way enhanced the value of Netcom's services to subscribers or attracted new subscribers. 907 F. Supp. at 1377. But see Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996) (holding that a plaintiff adequately stated a claim for vicarious liability against the operator of a flea market by alleging that defendants benefited financially from fixed daily rental fees paid by each infringing vendor, and rejecting defendant's argument that the financial benefit prong of the test for vicarious liability could only be satisfied if the defendant earned a commission directly tied to the sale of particular infringing item).

h. Netcom's First Amendment argument

(1) Chilling effect on Internet access providers. Netcom argued that plaintiffs' theory of liability would chill the use of the Internet and therefore contravene the First Amendment. Judge Whyte agreed in dicta that there could be a serious chilling effect if Usenet servers were responsible for all messages coming through their systems, but he wrote that he was "not convinced that Usenet servers are directly liable for causing a copy to be made, and absent evidence of knowledge and participation or control and direct profit, they will not be contributorily or vicariously liable." He further wrote that "[t]he copyright concepts of the idea/expression dichotomy and the fair use defense balance the important First Amendment rights with the constitutional authority for 'promot[ing] the progress of science and the useful arts . . . .'" 907 F. Supp. at 1377.

(2) User liability: browsing as copyright infringement. Netcom also argued that plaintiffs' theory of liability would have a chilling effect on users, who could be found liable for copyright infringement merely by browsing infringing works. Judge Whyte wrote in dicta that browsing "technically causes an infringing copy of the digital information to be made in the screen memory" since under MAI Systems Corp. v. Peak Computer, Inc., 911 F.2d 511 (9th Cir. 1993) (supra § I(A)(2)(b)(1)), cert. dismissed, 510 U.S. 1033 (1994), a copy is fixed when information is temporarily placed in RAM, including in the case of

browsing, screen RAM. Judge Whyte noted, however, that it was highly unlikely, as a practical matter, that a copyright owner could prove infringement by browsing, or would want to sue an individual browser. Judge Whyte also wrote that absent a commercial or profit-depriving use, digital browsing would be deemed a fair use. See supra § I(E)(8).

i. Netcom's fair use defense. The court found a material factual dispute on Netcom's entitlement to the fair use defense in light of evidence that, after it received notice, it knew that Erlich's use was infringing and had the ability to prevent its further distribution. See supra § I(E)(7)(c).

7. Netcom Settlement. In August 1996, the Church of Scientology reached agreement with Netcom to settle its copyright infringement action. As part of the settlement, Netcom announced new guidelines entitled "Intellectual Property Rights on the Internet," which are now distributed to all Netcom subscribers. The statement provides that computers whose host name or address includes "Netcom.com" are required to abide by Netcom's terms and conditions ("Terms"). The Terms include the prohibition on "using Netcom services to unlawfully distribute the intellectual property of others, regardless of format of property." The procedures for addressing postings challenged as improper are as follows:

1. The complainant shall provide Netcom and the posting party with notice of the alleged violation with enough specific detail to allow Netcom to locate the posting. The complainant shall ask the posting party to remove the material, pending Netcom's investigation.

2. Complainant shall substantiate its claim by providing Netcom with:

a. The copyright or trademark registration number;

b. A copy of the underlying work; and

c. A good faith certification, signed under penalty of perjury, the original work is the property of complainant, that a significant portion of that work has been copied, and that the use of the work is not defensible.

3. Upon receipt of notice from the complaining party, the posting party may provide Netcom with a response to the complaint.

4. While Netcom is investigating the complaint, Netcom will temporarily remove or deny access to the challenged material, to protect the rights of all involved.

5. If Netcom concludes that complainant has raised a legitimate claim, it will continue to deny access to the challenged material. If Netcom concludes that complainant has not raised a legitimate claim, Netcom will restore access to the challenged material.

8. Playboy Enterprises, Inc. v. Webbworld, Inc., 991 F. Supp. 543 (N.D. Tex. 1997), aff'd mem., 168 F.3d 486 (5th Cir. 1999).

a. Facts. Defendants owned or operated a website that offered subscribers, for a flat $11.95 monthly fee, access to sexually-oriented photographs and images, which they obtained from Usenet postings. Although none of the defendants themselves posted any images owned by plaintiff, one of the defendants had developed a software program which automatically searched news feeds which defendants received from pre-determined adult newsgroups, discarded most of the text, and retained sexually-oriented images. Images were then transformed into "thumbnail" copies, which allowed multiple photographs to be displayed on a single page and facilitated faster downloading (subscribers could then select larger versions of the thumb-nail prints, if they so desired). The images were then automatically transferred to defendants' website for subscriber viewing. Webbworld normally stored and displayed about 40,000 to 70,000 images at a given time, with approximately 5,000 to 10,000 images added (and an equal number deleted) daily. Images remained online for an average of six days. During the time WebbWorld was in operation, hundreds of plaintiff's copyrighted images appeared on the website.

b. Initial ruling. In an earlier ruling, Judge Dale Saffels, sitting by designation, entered summary judgement in favor of plaintiff on the issue of direct liability on all but 16 of the allegedly infringing images found on defendant's site (which defendants argued had been tampered with after downloading from their site). Judge Saffels also held defendants Bentley Ives and Benjamin Ellis vicariously liable. 968 F. Supp. 1171, 1175 (N.D. Tex. 1997).

c. Trial decision – direct liability. In a more detailed ruling following trial on the disputed works, Judge Barefoot Sanders rejected defendants' argument that any infringing images on their site would have existed on the Usenet, whether or not Webbworld had provided access to the images to its subscribers. The court also rejected defendants' attempt to compare themselves to a mere

conduit of information such as Netcom in Religious Technology Center v. Netcom On-Line Communication Services, Inc. 907 F. Supp. 1361, 1372-73 (N.D. Cal. 1995). In the words of the court, "Webbworld did not sell access; it sold adult images." Unlike in Netcom, Judge Sanders wrote that "Webbworld functioned primarily as a store . . . ," rather than "as a passive conduit of unaltered information." He wrote:

> Just as a merchant might re-package and sell merchandise from a wholesaler, so did Webbworld re-package (by deleting text and creating thumbnails) and sell images it obtained from various newsgroups. In contrast to the defendants in RTC, Webbworld took 'affirmative steps to cause the copies to be made'. . . . Such steps included using the ScanNews software to troll the Usenet for Webbworld's product.

d. Trial decision – vicarious liability. Judge Sanders, like Judge Saffels, found defendants Ives and Ellis vicariously liable. In rejecting the argument that defendants did not exercise control over the images automatically gathered and stored on its servers, the court wrote that "Webbworld exercised total dominion over the content of its site and the product it offered its clientele." The court in particular found significant the fact that defendants selected the newsgroups from which the images were automatically culled. For example, Judge Sanders noted that "a newsgroup named, for example, 'alt.sex.playboy' or 'alt.mag.playboy' might instantly be perceived as problematic from the standpoint of federal copyright law." The court further cautioned that:

> Webbworld might simply have refrained from conducting business until it had developed software or a manual system of oversight to prevent, or at least to minimize the possibility of, copyright infringement. . . . [H]aving developed and launched the ScanNews software for commercial use, Webbworld cannot now evade liability by claiming helplessness in the face of its "automatic" operation.

e. Vicarious of liability investors. The court declined to impose vicarious liability on a third defendant, James Gurkin, who contributed start-up capital to Webbworld and earned 25% of its net income. Although Gurkin derived financial benefit from the website the court found that he did not have the requisite supervisory authority over the infringing activity to justify the imposition of vicarious liability. Gurkin spent 3-5 hours per day

responding to customer emails, but had no access to the ScanNews software, had no decision-making authority and did not become a shareholder until late in the company's existence.

9. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

a. Facts. See supra § I(E)(5).

b. Contributory Liability. Having rejected the argument that Napster users were engaged in fair use, the Ninth Circuit concluded that the plaintiffs were likely to prevail against Napster on a theory of contributory infringement. Following Judge Whyte's landmark 1995 decision in Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995), the Ninth Circuit wrote that "if a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement."

The panel disagreed with (Chief) District Court Judge Patel's ruling that knowledge of "specific acts of infringement" did not have to be shown. It nonetheless found evidence of both actual and constructive knowledge. Actual knowledge was shown through (1) an internal document that spoke about "the need to remain ignorant of users' real names and IP addresses 'since they are exchanging pirated music'" and (2) the RIAA's notice, which informed Napster of the existence of more than 12,000 infringing files on its service.

Constructive knowledge, in turn, was shown because (1) Napster executives had recording industry experience; (2) Napster had enforced intellectual property rights in other instances; (3) Napster officials themselves downloaded copyrighted songs using the service; and (4) Napster promoted its service with screen shots that listed infringing files.

The panel emphasized, however, that it was not imputing the requisite level of knowledge to Napster to impose liability "merely because peer-to-peer file sharing technology may be used to infringe plaintiffs' copyrights." Moreover, it departed from the district court's conclusion that Napster failed to demonstrate that its system was capable of substantial noninfringing uses based on the percentage of current uses that were infringing.

c. Vicarious Liability. The court also ruled that plaintiffs were likely to prevail on their claim that Napster could be held vicariously liable for copyright infringement, which may be established where

a defendant has (1) a financial interest in the infringing activity and (2) the right and ability to supervise the conduct of direct infringers. In a ruling significant to many online sites, the Ninth Circuit concluded that the financial interest prong had been met even though Napster did not offer its service for a fee because "[f]inancial benefit exists where the availability of infringing material 'acts as a draw' for customers." In addition, the court noted that Napster's future revenues were directly dependent on increasing its user base.

With respect to Napster's right and ability to control the infringing conduct of its users, the Ninth Circuit wrote that the ability to block access "for any reason whatsoever" is evidence of the right and ability to supervise infringing conduct. In particular, the court cited as relevant Napster's terms of use in which it reserved the right to terminate accounts or refuse service. In this regard, the court's language may be viewed as overly broad. Not all providers of legitimate online services (such as traditional ISPs or backbone providers) *in fact* can control the conduct of thousands or even millions of users. Nor should such services be discouraged from adopting policies intended to penalize infringers.

By contrast, the Ninth Circuit's analysis should be viewed as having been heavily influenced by the fact that Napster itself created a system that was used overwhelmingly for acts of infringement and which it was uniquely able to control, access or block. The Ninth Circuit relied on internal documents that showed that Napster was – at best – willfully turning a blind eye to acts of infringement. The panel acknowledged, however, that Napster's ability to control the conduct of its users – like other online service providers – was "cabined by the system's current architecture." In the view of the Ninth Circuit, the district court failed to adequately account for "the boundaries of the premises that Napster 'controls and patrols' . . . ." At a minimum, however, the Ninth Circuit noted that Napster had the ability to locate infringing material listed on its indices and had the right to terminate users' access to its system.

d. Implied License, Copyright Misuse and First Amendment Defenses. The Ninth Circuit rejected various defenses including waiver, implied license and copyright misuse. The court also rejected Napster's claimed First Amendment right to publish its directory and that of its users to exchange information.

e. The District Court's Injunction. Despite its analysis of Napster's likely liability, the Ninth Circuit concluded that the scope of the district court's injunction should be modified because contributory

infringement could only be established where Napster (1) received "reasonable knowledge" of specific infringing files with copyrighted musical compositions and sound recordings; (2) knew or should have known that such files were available on the Napster system; and (3) failed to act to prevent viral distribution of the works. In the words of the panel, "[t]he mere existence of the Napster system, absent actual notice and Napster's demonstrated failure to remove the offending material, is insufficient to impose contributory liability." The district court's original ruling, by contrast, was found to be overly broad because it placed on Napster the entire burden of ensuring that no copying, downloading, uploading, transmitting or distribution of plaintiffs' works occurred on its system.

The Ninth Circuit concluded that plaintiffs bore the initial burden of providing notice to Napster of the copyrighted works and files containing such works on its system *before* Napster had any duty to disable access to the infringing material. Napster, however, also was under a duty according to the Ninth Circuit, to police its service "within the limits of the system." The court recognized that "this is not an exact science in that the files are user named."

f. Judge Patel's order on remand. On remand, Judge Patel enjoined Napster from engaging in, or facilitating others in, copying, downloading, uploading, transmitting, or distributing copyrighted sound recordings and set forth a specific set of procedures to be followed to effectuate that result, consistent with the shifting burdens of proof outlined in the Ninth Circuit's ruling. First, plaintiffs were ordered to provide Napster with notice of their copyrighted sound recordings. Notice was required to include the title of the work, the name of the featured recording artist promoting the work, certification that plaintiffs own or control the rights allegedly infringed and the name(s) of *one or more* files available on the Napster system that included the work.

Judge Patel further ruled that all parties must use reasonable measures to identify variations of the file names or spellings of song titles or artist names. She wrote that "[i]f it is reasonable to believe that a file available on the Napster system is a variation of a particular work or file identified by plaintiffs, all parties have an obligation to ascertain the actual identity (title and artist name) of the work and to take appropriate action" within the context of the order.

Given the transitory nature of files transferred over the Napster service and the ease with which Napster could search its own service at any given time for specific works, Judge Patel concluded

that it would be sufficient for the plaintiffs to simply identify a song and the location of *one or more* files containing the work, in order to shift the burden on Napster to search the files on its system "against lists of copyrighted recordings provided by plaintiffs." This process would, according to Judge Patel's order, provide Napster with "reasonable knowledge of specific infringing files" as required by the Ninth Circuit.

Once Napster received "reasonable knowledge" through notice, reasonable measures to identify file variations or searching its own system for files matching the list provided by plaintiffs, Napster then would have three (3) business days to "prevent such files from being included in the Napster index (thereby preventing third party access to the files corresponding to such names through the Napster service)." Napster was also ordered to "prevent the downloading, uploading, transmitting or distributing of the noticed copyrighted sound recordings."

g. Pre-release recordings. Judge Patel's order also addressed pre-release versions of sounds recordings. Specifically, she ruled that:

> Plaintiffs may provide to Napster in advance of release the artist name, title of the recording, and release date of sound recordings for which, based on a review of that artist's previous work, including but not limited to popularity and frequency of appearance on the Napster system, there is a substantial likelihood of infringement on the Napster system. Napster shall begin with the first infringing file block access to or through its system to the identified recording. As Napster presently has the capability (even without enhancing its technology) to store information about and subsequently screen for a particular recording, the burden is far less and the equities far more fair to require Napster to block the transmission of these works in advance of their release. To order otherwise would allow Napster a free ride for the length of time it would take plaintiffs to identify a specific infringing file and Napster to screen the work.

h. 2002 Ninth Circuit Ruling. In A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002), the Ninth Circuit upheld the lower court's modified preliminary injunction order, which had obligated Napster to remove any user files from its music index if it had "reasonable knowledge" that the file contained one or more of plaintiffs' works and obligated plaintiffs to provide Napster with notice of specific infringing files (including the name of the performing artist, title of the work, certification of ownership and

the name(s) of one or more files containing the work that had been on Napster's index). The Ninth Circuit also upheld the district court's order compelling Napster to use a new, more effective filtering mechanism (one that used audio fingerprinting technology, which was not vulnerable to textual variations in file names) and shut down its service until every effort was made to "get zero tolerance . . . ."

10. In re: Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003).

a. Facts. Aimster, which like Napster, was a "file sharing" service, provided its users with software that allowed them to conceal their identity and transfer encrypted MP3 files through instant messaging services such as AOL's IM, facilitating the creation of a peer-to-peer (or user-to-user) network. The software also allowed users to identify each other and locate files they might want to copy.

b. Ruling. The Seventh Circuit affirmed the entry of a preliminary injunction based on the finding that plaintiffs were likely to prevail on their claim for contributory copyright infringement.

c. Knowledge (contributory infringement). The district court had found that the plaintiffs were likely to prevail in showing that Aimster had actual knowledge because (1) plaintiffs repeatedly sent notices identifying copyrighted works accessible on Aimster; (2) Aimster's Guardian Tutorial, posted on Aimster's website, "demonstrated how to infringe Plaintiff[s'] copyrights by using specific copyrighted titles as pedagogical examples."; and (3) Club Aimster actually tracked the most popular songs available over the service and "not only provides users with an easy way to locate and download copyrighted material, but it even makes reference to where each particular song is ranked on the Aimster list vis-a-vis the music labels' lists." In addition, the Seventh Circuit noted that there was no evidence that Aimster in fact had been used for non-infringing purposes.

d. Applicability of the *Sony* Defense (substantial non-infringing uses). Judge Posner offered an extended analysis of Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984), writing that "[e]ven when there are noninfringing uses of an Internet file-sharing service, if the infringing uses are substantial then to avoid liability as a contributory infringer the provider of the service must show that it would have been disproportionately costly for him to eliminate or at least reduce substantially the infringing uses."

e. Use of encryption. Judge Postner wrote that by allowing users to encrypt files, Aimster "must take responsibility for that self-inflicted wound." Although encryption *per se* will not lead to liability, he wrote that "a service provider that would otherwise be a contributory infringer does not obtain immunity by using encryption to shield itself from actual knowledge of the unlawful purposes for which the service is being used."

11. In MGM Studios, Inc. v. Grokster, Ltd., 380 F.3d 1154 (9th Cir. 2004), the Ninth Circuit affirmed the entry of summary judgment for the defendant P2P services on plaintiffs' claims for contributory infringement and vicarious liability. The court did not address the potential liability of Sharman Networks, the proprietor of the kazaa.com website and Kazaa Media Desktop. Likewise, the order only addressed the then-current versions of Grokster's and StreamCast's products and services (rather than earlier versions, for which plaintiffs sought damages but not injunctive relief). The case presently is before the U.S. Supreme Court.

a. Facts. Defendants Grokster, StreamCast and Kazaa BV independently branded, marketed and distributed "file sharing" software. Originally, all three companies used FastTrack networking technology, which allowed users of the three software platforms to connect to what essentially was a single peer-to-peer network and to exchange files seamlessly on all three systems. At the time of the motion, StreamCast used Gnutella technology and Grokster distributed its own software – Morpheus – in lieu of a branded version of the Kazaa Media Desktop. The lower court had written that "[a]lthough novel in important respects, both the Grokster and Morpheus platforms operate in a manner conceptually analogous to the Napster system . . . ."

b. Contributory infringement – 2 part test. The Ninth Circuit adopted a new test for contributory infringement, determining that a court must first evaluate if a product is capable of "substantial" or "commercially significant" noninfringing uses, as those terms were used in Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).

(1) If a product does not have substantial or commercially significant noninfringing uses, a plaintiff may establish liability by showing that the defendant had actual or contructive knowledge.

(2) If a product has such uses, a copyright owner must determine that the defendant, in the context of a P2P system, "had reasonable knowledge of specific infringing

files and failed to act on that knowledge to prevent infringement."

c. In *Grokster,* the Ninth Circuit found that the defendants' services were capable of substantial noninfringing uses, notwithstanding the fact (as noted in a footnote) that evidence was presented that 90% or more of the files on defendants' networks at the relevant time period were infringing. The Ninth Circuit emphasized that the relevant inquiry focused on the *potential* for substantial or commercially significant uses, not necessarily actual use. The Ninth Circuit also concluded that 10% noninfringing use was significant because as an absolute number this percentage represented hundreds of thousands of files. This aspect of the court's decision is inconsistent with Judge Posner's analysis in In re Aimster Copyright Litig., 334 F.3d 643, 651 (7th Cir. 2003).

d. The Ninth Circuit found that the defendants could not be held liable for contributory infringement because they did not have specific knowledge of individual file exchanges at the moment in time when they occurred. In so ruling, the appellate court sided with District Court Judge Wilson's analysis that "plaintiffs' notices of infringing conduct are irrelevant if they arrive when Defendants do nothing to facilitate, and cannot do anything to stop, the alleged infringement." In his earlier opinion, Judge Wilson had dismissed what he conceded was "a massive volume" of evidence similar to what was presented in the *Napster* case – including documents suggesting that defendants marketed themselves as "the next Napster," that various searches were performed by defendants' executives for copyrighted song titles or artists, that various internal documents revealed that defendants were aware that their users were infringing copyrights and that the plaintiffs sent defendants thousands of notices regarding alleged acts of infringement – because plaintiffs could not show that defendants had "actual knowledge of infringement at a time when they can use that knowledge to stop the particular infringement."

Judge Wilson had earlier cast the question of whether defendants materially contributed to the infringing conduct of their users in terms of whether they could "do anything, aside from distributing software, to actively facilitate – or whether they could do anything to stop – their users' infringing activity." He had placed great significance on the fact that unlike Napster, where files were indexed on a central server, defendants did not provide the "site and facilities" for direct infringement. Judge Wilson wrote that "[i]f either Defendant closed their doors and deactivated all computers within their control, users of their products could continue sharing files with little or no interruption."

e. Vicarious infringement. The Ninth Circuit concluded that the defendants could not be held vicariously liable because they did not have the ability to control user conduct (because of the decentralized nature of the peer-to-peer system created by the software applications they distributed). The district court had earlier found that defendants had a financial interest in their services because they derived substantial revenue from advertising (StreamCast, for example, generated $1.8 million from advertisements in 2001 and projected earnings of $5.7 million for 2002).

f. Significance of the decision. An analysis of this case is set forth in Ian C. Ballon, "Ninth Circuit's *Grokster* Decision Changes the Law of Secondary Copyright Liability," *California Copyright Conference Newsletter*, Sept. 2004. The case presently is before the U.S. Supreme Court.

12. In Arista Records, Inc. v. MP3Board, Inc., 00 Civ. 4660 (SHS), 2002 U.S. Dist. LEXIS 16165 (S.D.N.Y. Aug. 28, 2002), the court denied plaintiffs' motion for summary judgment against a service that provided links to sites that made available MP3 files, where the court found that material issues of fact existed on the question of whether any direct infringement actually occurred with the aid of the MP3Board site. The court also denied defendant's motion for summary judgment, finding that all four fair use factors weighed against MP3Board. In addition to having established links to sites that offered MP3 downloads, the MP3Board site solicited additional links from its users and provided a link to Freedrive, where users could store audio files online. The service also included a message board. In response to user posts, MP3Board personnel personally searched for links to songs and then them on the message board, solicited other users to provide the requested works and obtained and posted passwords to enable users to access particular music files.

G. Liability Limitations Under the Digital Millennium Copyright Act

1. Copyright Liability Limitations. The Online Copyright Infringement Liability Limitation Act incorporated as Title II of the Digital Millennium Copyright Act limits the liability of "Service Providers" (which as broadly defined under the Act would include ISPs, OSPs, search engines, portals and even owners of corporate intranets) for third party liability for damages, costs or attorney's fees under the Copyright Act, but only if an entity complies with a series of technical requirements. A Service Provider that satisfies three threshold prerequisites set forth in 17 U.S.C. § 512(I) (discussed below) may be entitled to immunity from copyright infringement liability for (1) transmitting, routing, and providing connections to infringing material (or what the statute refers to as "transitory digital network communications"); (2) system caching;

(3) information stored by a user (the "user storage" limitation); or
(4) linking or referring users to infringing material (the "information location tools" limitation).

2. Exemption from Liability (under any theory of law) for Removing or Disabling Access to Content. A Service Provider that otherwise has met the threshold requirements set forth in section 512(I) may be entitled to a broad exemption from liability under any theory of recovery for any good faith act to disable access to or remove material believed to be infringing, regardless of whether the material or activity is ultimately determined to be infringing.

   There is one exception to the broad exemption provided for removing or blocking access to content. If a Service Provider receives a notification about allegedly infringing material stored at the direction of a subscriber, it must comply with the specific requirements of subparts (c)(3) and (g)(2) governing notification and counter notification in order to avoid all potential liability. Specifically, a Service Provider would have to satisfy the requirements of subpart (c)(3) to limit its potential liability to the copyright owner for infringement and comply with subpart (g)(2) to avoid any liability to its subscriber for disabling access to or removing content in response to a notification.

3. Threshold Requirements. In order to benefit from any of the new liability limitations created by the Act, a Service Provider must adopt and implement a policy of terminating the accounts or subscriptions of repeat infringers; inform subscribers and account holders of this policy; and accommodate and not interfere with "standard technical measures." To benefit from the user storage, caching and information location tools limitations, Service Providers also will need to designate agents to receive notification of alleged acts of infringement and comply with specific rules for removing or blocking access to content alleged to be infringing. For information on agent designation, see Designation of Agent to Receive Notification of Claims Infringement, 63 Fed. Reg. 59233 (Nov. 3, 1998). Further, to avoid liability to subscribers in cases where content is removed in response to a notification, Service Providers must comply with procedures governing counter notifications and potentially replace or restore access to content removed in response to a notification.

4. Procedures for Notification and Counter Notification. Where a Service Provider seeks to benefit from all liability limitations and the one exemption created by the Act, its agent must be prepared to act swiftly in response to Notifications and Counter Notifications. When a Notification that substantially complies with the requirements of the statute is received, a Service Provider must expeditiously remove or block access to the allegedly infringing content. Where a subscriber posted the content, the Service Provider must promptly notify its subscriber that it has removed or

disabled access to the material. If the subscriber serves a Counter Notification on the agent, the Service Provider must promptly provide the original complainant with a copy of the Counter Notification. The Service Provider must then replace or restore access to the disputed content between the 11th and 14th business day after the date on which it received the Counter Notification unless, within the first 10 business days, it receives a notice from the original complainant that it has filed suit to restrain the subscriber from engaging in infringing activity (in which case the Service Provider must take no further action pending a ruling by the court). Service Providers and other affected parties may recover damages if material misrepresentations are made in either Notifications or Counter Notifications.

5. Safe harbor protection is presumptive, not automatic, and is only available to service providers that can prove they do not have actual or constructive knowledge of infringement. See ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619 (4th Cir. 2001).

6. Benefits for Service Providers. Service Providers that choose to comply with the Act may limit their liability for acts of third party copyright infringement (although not the acts of their employees, unless the Service Provider is also a Nonprofit Educational Institution as defined under the Act) and may avoid liability for removing or disabling access to content believed in good faith to be infringing. Compliance may be time consuming, burdensome and costly for some companies, however, especially where Service Providers seek to benefit from the exemption for removing content (which requires them to meet tight time restrictions for forwarding Notifications to subscribers and responding to Counter Notifications).

7. Benefits for Copyright Owners. Copyright owners may be able to obtain the extra-judicial remedy of having infringing content removed from the Internet at a fraction of the cost of litigation if they understand the Act and know how to benefit from it. They also may be able to obtain the quick and inexpensive identification of the identity of alleged infringers who act pseudonymously. Copyright owners must understand and be prepared to respond within the tight time constraints imposed by the Act and how to properly draft substantially complying Notifications. Otherwise, copyright owners may needlessly incur substantial litigation fees to obtain relief that could be obtained from Service Providers who choose to comply with the Act virtually free of charge.

8. Service Provider Obligations in Response to Notifications.

   a. In ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619 (4th Cir. 2001), the Fourth Circuit ruled that a copyright owner substantially complied with the requirement that it provide a

"representative list" of infringing material as well as information "reasonably sufficient" to enable the service provider to locate infringing material by (1) identifying two USENET groups (*alt.als* and *alt.binaries.pictures.erotica.als*) that it alleged had been created solely for the purpose of publishing ALS Scan's copyrighted works, (2) asserting that virtually all of the images on the two newsgroups were infringing (and noting that such images includes ALS Scan's name and/or a copyright symbol), and (3) referring the service provider to two URLs where it could find copies of the genuine works and obtain copyright information.

b. In Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082 (C.D. Cal. 2001), a district court granted eBay's motion for summary judgment in a case where the copyright owner failed to authenticate a notification by including a written statement under penalty of perjury substantiating the accuracy of the notification or certifying that he had "a good faith belief that the use of the material in the manner complained of" was unauthorized.

c. In Ellison v. America Online, Inc., 357 F.3d 1072 (9th Cir. 2004), the Ninth Circuit found there was a triable issue of fact on the issue of whether AOL met the threshold requirements of the DMCA's liability limitation provisions, in a case involving USENET posts, where AOL had changed the email address used for submitting DMCA notifications but had briefly failed to either forward or return communications sent to the old address, including the notice at issue in the suit.

d. In Costar Group, Inc. v. Costar Realty Information, Inc., 164 F. Supp. 2d 688 (D. Md. 2001), the court denied cross-motions for summary judgment under the DMCA, finding that whether (1) removal of infringing material was expeditious or (2) termination of repeat offenders was reasonable and effective constituted material issues precluding summary judgment.

e. In Hendrickson v. Amazon.com, Inc., 298 F. Supp. 2d 914 (C.D. Cal. 2003), the court ruled that, to be effective, a notification must relate to material actually on a site at the time it is sent and does not impose on service providers a continuing obligation to monitor their sites for potentially infringing material that may be posted at a later date.

f. In Rossi v. Motion Picture Association of America, Inc., No. 03-16034, 2004 U.S. Dist. LEXIS 24743 (9th Cir. Dec. 1, 2004), the Ninth Circuit affirmed the entry of summary judgment for the defendant-copyright owner on state tort law claims for tortious interference with contractual relations, tortious interference with

prospective economic advantage, libel and defamation, and intentional infliction of emotional distress. In that case, the court had held that the copyright owner had complied with the procedures of the DMCA based on a "good faith belief" that the plaintiff's Web site had included infringing copies of its protected motion pictures (based on plaintiff's own representations on the site).

9. Service Provider Subpoenas (17 U.S.C. § 512(h))

In RIAA v. Verizon Internet Services, 351 F.3d 1229 (D.C. Cir. 2003), the D.C. Circuit granted Verizon's motion to quash a DMCA subpoena (served to identify pseudonymous alleged infringers), finding that section 512(h) did not authorize the issuance of a subpoena to a service provider acting solely as a conduit for communications not actually stored on its own servers.

10. More Information. For more information on the Digital Millennium Copyright Act, see Ian C. Ballon, *E-Commerce and Internet Law - A legal Treatise with Forms* § 8.12 (Glasser LegalWorks 2004 Cum. Supp.).

H. Republication of Digital Content in Databases

1. Copyright Protection for Databases and other compilations, such as newspapers, potentially may be subject to two separate copyrights. 17 U.S.C. § 230(c) provides that a copyright in a contribution to a collective work is distinct from the collective work itself. In the absence of an express transfer of the copyright or any rights under it, the owner of the copyright in the collective work is presumed to have acquired only the privilege of reproducing and distributing the contribution "as part of that collective work, any revision of that collective work, and any later collective work in the same series."

2. In New York Times Co. v. Tasini, 533 U.S. 483 (2001), the U.S. Supreme Court ruled that a digitized version of *The New York Times* constituted a new work, not a permissible revision under 17 U.S.C. § 201(c), for which separate permission was required from individual freelance writers who had not expressly granted the newspaper all electronic rights.

3. Impact. The *Tasini* opinion potentially affects individual contributions to collective works first published after January 1, 1978, when the 1976 Copyright Act took effect. Most publishers and database owners responded to the Tasini decision by purging freelance material from their databases. A subsequent lawsuit by Mr. Tasini to prevent the New York Times from removing freelance content from its databases in response to the U.S. Supreme Court's ruling was dismissed for lack of jurisdiction. See Tasini v. New York Times, 184 F. Supp. 2d 350 (S.D.N.Y. 2002).

4. License grants. Today, collective works owners and publishers typically demand contractual grants including electronic rights or "rights in all media now known or hereinafter created."

5. Class action litigation. The potential liability of database owners for copyright infringement based on New York Times Co. v. Tasini is the subject of pending putative class action lawsuits that have been consolidated by the MDL Panel as In re Literary Works in Electronic Databases Copyright Litigation, MDL No. 1379 (S.D.N.Y).

6. Greenberg v. National Geographic Society, 244 F.3d 1267 (11th Cir.), cert. denied, 534 U.S. 951 (2001). The Eleventh Circuit ruled that the National Geographic's repackaging of earlier editions onto a CD ROM set – comprised of (1) digitally reproduced issues of the magazine; (2) software that served as the storage retrieval system; and (3) a moving cover sequence that reproduced one of the plaintiff-freelance photographer's images as part of an animated clip at the beginning of each disk – constituted a new work, rather than a "later collective work in the same series" within the meaning of 17 U.S.C. § 201(c). Among other things, the court cited the National Geographic's own characterization of the work in its copyright registration application. The court rejected the defendant's fair use defense in part because the use of the plaintiff's image in the moving cover sequence "effectively diminished, if not extinguished, any opportunity [he] . . . might have had to license the photograph to other potential users."

7. By contrast, in Faulkner v. National Geographic Society, 294 F. Supp. 2d 523 (S.D.N.Y. 2003), the court ruled that the publisher of the National Geographic was privileged under section 201(c) to market a digital archive of its past issues on CD-ROM and DVD on the theory it was a revision, not a new work, because it was a package that contained everything that made the magazine copyrightable as a collectice work and was readily recognizable as a variation of the original.

8. In Random House, Inc. v. Rosetta Books LLC, 283 F.3d 490 (2d Cir. 2002), the Second Circuit affirmed the lower court's denial of Random House's motion to enjoin an Internet publisher from selling certain works as "e-books." Random House's publishing contracts with the affected authors granted it the right to "print, publish and sell the works in book form." The district court had concluded that the plaintiff was unlikely to prevail by showing that these contracts extended to publication in digital format.

9. Common law protections. Database owners have sought to protect factual databases that otherwise may be entitled to only "thin" copyright protection through common law remedies, including trespass. See infra § III(H).

10. Additional Information. For a more complete analysis of database law, See Ian C. Ballon, *E-Commerce and Internet Law - A legal Treatise with Forms,* Chapter 9 (Glasser LegalWorks 2001).

I. Criminal Copyright Infringement. Criminal copyright infringement may be found if more than $1,000 worth of copies are made in any 180-day period.

J. First Amendment and Public Domain Issues.

1. The U.S. Supreme Court rejected First Amendment and Copyright Clause Constitutional challenges to the Sonny Bono Copyright Term Extension Act in Eldred v. Ashcroft, 537 U.S. 186 (2003).

2. In Dastar Corp. v. Twentieth Century Fox Film Corp., 539 U.S. 23 (2003), the U.S. Supreme Court ruled that a company that marketed a video of a television program that had come into the public domain, claiming it as its own and not designating the true origin of the program, could not be held liable under the Lanham Act for false designation of origin because the work was no longer protectable under copyright law.

K. Pop Up Ads. See infra § II(E).

II. TRADEMARK AND TRADE DRESS PROTECTION IN CYBERSPACE

A. Direct and Third Party Trademark Infringement on the Internet

1. Elements of an infringement claim.

a. To prevail on a claim for trademark infringement, a plaintiff must show (1) a protectable mark; and (2) likelihood of confusion as to the origin, affiliation or sponsorship of the defendant's product. See, e.g., Goto.com, Inc. v. The Walt Disney Co., 202 F.3d 1199 (9th Cir. 2000) (logo infringement on a website).

b. To be protectable, a mark must be inherently distinctive or have acquired secondary meaning. E.g., A.J. Canfield Co. v. Honickman, 808 F.2d 291, 296-97 (3d Cir. 1986).

(1) A mark is "inherently distinctive" if it is fanciful, arbitrary or suggestive. Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763 (1992).

(2) A descriptive term, in contrast to one that is inherently distinctive, is entitled to trademark protection only if it has acquired secondary meaning. E.g., A.J. Canfield Co. v. Honickman, 808 F.2d 291, 296-97 (3d Cir. 1986). To prove secondary meaning, a plaintiff must show an association between an alleged mark and the product in the minds of

relevant consumers. E.g., Nutri/System, Inc. v. Con-Stan Indus., 809 F.2d 601, 605 (9th Cir. 1987)

(3) Generic terms are never protectable. A.J. Canfield Co. v. Honickman, supra, 808 F.2d at 296-97.

c. Likelihood of confusion is determined by a balancing test. The following factors are relevant: (1) strength of the mark; (2) proximity of the goods; (3) similarity of the marks; (4) evidence of actual confusion; (5) marketing channels used; (6) type of goods and the degree of care likely to be exercised by the purchaser; (7) defendant's intent in selecting the mark; and (8) likelihood of expansion of the product lines. E.g., AMF Inc. v. Sleekcraft Boats, 599 F.2d 341, 348-49 (9th Cir. 1979).

2. Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993).

a. Facts: See supra § I(F)(4)(a). Frena operated a BBS on which subscribers uploaded and downloaded digitized copies of photographs from Playboy magazine. The original text was removed from the photographs and defendant's name, BBS name and telephone number was placed on each photograph. In addition, the trademarks "PLAYBOY" and "PLAYMATE" were used in file descriptions for 170 of the images. Defendant argued that the subscribers who uploaded the images provided the file descriptions. He also argued that he was unaware of the infringements and had allowed subscribers to upload anything they wanted on the BBS.

b. Trademark infringement — file descriptors. The court granted partial summary judgment for plaintiff, noting that bad faith need not be shown to establish trademark infringement under 15 U.S.C. § 1141(a). 839 F. Supp. at 1560-61.

c. Unfair competition. The court granted partial summary judgment for plaintiff on its unfair competition claim, finding that Frena's deletion of plaintiff's text from the photographs, addition of his own text to some of the images and appropriation of Playboy's photographs without attribution constituted acts of unfair competition under 15 U.S.C. § 1125(c). By falsely inferring and describing the origin of the photographs, Frena made it appear that Playboy Enterprises, Inc. authorized Frena's product. 839 F. Supp. at 1562.

d. Reverse "passing off." The court also held that Frena's removal of Playboy's trademarks from the photographs constituted "reverse passing off." Id.

3. Sega Enterprises Ltd. v. MAPHIA, 857 F. Supp. 679 (N.D. Cal. 1994).

a. Facts: See supra § I(F)(5)(a). Plaintiff's "Sega" trademark appeared on the screen whenever a game that had been downloaded from the MAPHIA bulletin board was subsequently played. Some of the bootlegged programs posted on the bulletin board did not function as smoothly as genuine, commercially available Sega games, either because they were pre-release versions of games not yet commercially available, or because glitches had been introduced in the copying process. Id. at 684. The court concluded that bulletin board users and/or parties who may receive copies from the bulletin board "are likely to confuse the unauthorized copies downloaded and transferred from the MAPHIA bulletin board with genuine Sega videogame programs." Id.

b. Holding: preliminary injunction granted in part based on a finding of trademark infringement. The court reasoned that "confusion, if not on the part of bulletin board users, is inevitable on the part of third parties who may see the copied games after they enter the stream of commerce." Id. at 688. In a subsequent opinion granting summary judgment in favor of Sega, the court emphasized that, as in Playboy Enterprises, Inc. v. Frena, the defendant "adopted the use of the Sega name as file descriptors on his BBS and the SEGA logo within those games, because he knew about the [infringing] use, and tacitly authorized it. Additionally, [defendant] used the mark when he created the file area that used the name Sega to identify the area where the game files would be located." 948 F. Supp. 938 (N.D. Cal. 1996).

c. False designation of origin: The court also found Sega likely to prevail on its unfair competition claim under the Lanham Act based on its finding that the public is likely to be deceived or confused by the similarity of marks shown on both the genuine product and the bootlegged programs uploaded to MAPHIA. 857 F. Supp. at 688.

4. Contributory trademark infringement

a. Contributory trademark infringement may be found if a defendant (1) intentionally induces another to infringe a trademark, or (2) continues to supply a product knowing that the recipient is using the product to engage in trademark infringement. Inwood Laboratories, Inc. v. Ives Laboratories, Inc., 456 U.S. 844, 854-55 (1982); Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996); Ian C. Ballon, Pinning the Blame in Cyberspace: Towards A Coherent Theory for Imposing Vicarious Copyright,

Trademark and Tort Liability for Conduct Occurring Over the Internet, 18 Hastings J. Communications & Ent. L. 729, 750-53, 761-64 (1996).

b. No liability for offering an Internet-related service. In Lockheed Martin Corp. v. NSI, 194 F.3d 980 (9th Cir. 1999), the Ninth Circuit ruled that a domain name registrar could not be held contributorily liable for registering infringing domain names after receiving two cease and desist letters because a registrar supplies a service – not a product – to third parties.

c. Actual knowledge. Two lower courts have ruled that a domain name registrar cannot be deemed to have received actual or constructive notice of an infringement merely because it was sent a cease and desist letter because of the inherent uncertainty in defining the scope of an owner's rights in a mark (which typically expand or contract over time). See Lockheed Martin Corp. v. NSI, 985 F. Supp. 949 (C.D. Cal. 1997), aff'd on other grounds, 194 F.3d 980 (9th Cir. 1999); Academy of Motion Picture Arts and Sciences v. NSI, 989 F. Supp. 1276 (C.D. Cal. 1997).

B. Dilution in Cyberspace

In January 1996, Congress passed the Federal Trademark Dilution Act, which is intended to protect famous marks, and does not require a showing of likelihood of confusion (or even that the plaintiff and defendant are competitors of one another).

1. Elements of A Claim. The owner of a famous mark shall be entitled, "subject to the principles of equity and on such terms as the court deems reasonable," to an injunction against another person's commercial use of a mark or trade name, if such use begins after the plaintiff's mark has become famous and causes dilution of the distinctive quality of the mark. 15 U.S.C. § 1125(c)(1).

2. Dilution Defined. Dilution is defined as "the lessening of the capacity of a famous mark to identify and distinguish goods or services, regardless of the presence or absence of – (1) competition between the owner of the famous mark and other parties, or (2) likelihood of confusion or mistake or to deceive." 15 U.S.C. § 1127. Among other things, dilution may be shown by evidence of blurring or tarnishment.

   a. Blurring. Dilution may be shown by blurring. See, e.g., I.P. Lund Trading ApS & Kroin, Inc. v. Kohler Co., 163 F.3d 27, 49-50 (1st Cir. 1998).

b. Tarnishment. Tarnishment typically is shown when a famous mark is associated with hard core pornography, spamming or cybersquatting.

(1) Hasbro, Inc. v. Internet Entertainment Group Ltd., Case No. C96-139 (W.D. Wash. Feb. 5, 1996). In a suit brought by Hasbro, Inc., which owns the trademark "Candy Land," the court enjoined the defendant's use of the domain name *candyland.com* for a porno site. In addition to *candyland.com*, the defendant had reserved the domain name *parkerbrothers.com*, which plaintiff's counsel argued evidenced the defendant's intent to trade on plaintiff's wholesome image as the manufacturer of board games for children. "Washington Judge Enjoins Use of Trademark as Internet Domain Name," Mealey's Litigation Reports: Intellectual Property, Mar. 18, 1996.

(2) In Toys R Us v. Akkaoui, Case No. C 96-3381 CW, 1996 U.S. Dist. LEXIS 17090 (N.D. Cal. Oct. 29, 1996) plaintiff Geoffrey Inc., owner of a family of marks ending in "R Us" (including Toys R Us, in use since 1960, and Kids R Us, in use since 1983) brought suit against Mohamad Ahmad Akkaoui, Lingerienet and Acme Distributors, which operated an Internet service offering sexual devices and clothing under the adultsrus.com domain name and Adults R Us mark. In entering a preliminary injunction, Judge Claudia Wilken of the Northern District of California determined that plaintiff's marks are distinctive and famous and that defendants' use of Adults R Us was likely to tarnish plaintiff's marks by associating them with sexual goods inconsistent with the wholesome image plaintiff sought to cultivate in the marketplace. But see Toys "R" Us, Inc. v. Feinberg, 26 F. Supp. 2d 639 (S.D.N.Y. 1998) (holding that the use of the *gunsrus.com* domain name by a Massachusetts gun dealer on a website entitled "Guns Are We" neither tarnished nor blurred plaintiff's marks), rev'd on procedural grounds, 201 F.3d 432 (2d Cir. 1999).

(3) In America Online, Inc. v. IMS, 24 F. Supp. 2d 548, 552 (E.D. Va. 1998), the court found that a famous mark could be diluted when used as a phony return email address in connection with unsolicited commercial email (or spam).

3. Distinctive and Famous Marks. In determining whether a mark is "distinctive and famous," a court "may consider factors such as, but not limited to" – (A) the degree of inherent or acquired distinctiveness of the mark; (B) the duration and extent of use of the mark in connection with

the goods or services with which the mark is used; (C) the duration and extent of advertising and publicity of the mark; (D) the geographical extent of the trading area in which the mark is used; (E) the channels of trade for the goods or services with which the mark is used; (F) the degree of recognition of the mark in the trading areas and channels of trade used by the marks' owner and the person against whom the injunction is sought; (G) the nature and extent of use of the same or similar marks by third parties; and (H) whether the mark was registered on the principal register or under the 1881 or 1905 Trademark Acts. 15 U.S.C. § 1125(c)(1).

a. Niche market fame. Some courts have ruled that a mark may be considered famous and distinctive within a narrow market if it is the same market within which the defendant operates. See Times Mirror Magazines, Inc. v. Las Vegas Sporting News, 212 F.3d 157, 164-65 (3d Cir. 2000), cert. denied, 513 U.S. 1071 (2001); Advantage Rent-A-Car v. Enterprise Rent-A-Car, 238 F.3d 378, 380 (5th Cir. 2001); Syndicate Sales, Inc. v. Hampshire Paper Corp., 192 F.3d 633, 640-41 (7th Cir. 1999) (summarizing and harmonizing divergent lower court decisions).

b. Descriptive Marks. In TCPIP Holding Co. v. Haar Communication Inc., 244 F.3d 88 (2d Cir. 2001), the Second Circuit held that descriptive marks that have acquired secondary meaning are not entitled to protection under the Federal Trademark Dilution Act. This holding appears to contradict the clear legislative intent that "a mark may be deemed 'famous' even if not inherently distinctive, that is, even if the mark is not arbitrary, fanciful or coined." See Ian C. Ballon, *E-Commerce and Internet Law – A Legal Treatise With Forms* § 10.11, at 10-87 (Glasser LegalWorks 2001) (citing the legislative history).

4. Proof Required. The U.S. Supreme Court, resolving a split in the circuits, ruled in Moseley v. V Secret Catalogue, Inc., 537 U.S. 418 (2003) that a trademark owner must show evidence of actual dilution, rather than merely likelihood of dilution, to obtain injunctive relief.

5. Defenses. The following are complete defenses to a dilution claim (15 U.S.C. §§ 1125(c)(3) and 1125(c)(4)):

a. Defendant's ownership of a valid registration under the 1881 or 1905 Trademark Acts or on the principal register;

b. Fair use of a famous mark in a comparative commercial advertisement or promotion to identify competing goods or services;

c. Noncommercial use of the mark; and

d. All forms of news reporting and news commentary.

6. Relief. The Act affords the owner of a famous mark the right to obtain injunctive relief and, in cases where the defendant willfully intended to trade on the owner's reputation or to cause dilution of the mark, damages, attorneys' fees and destruction of goods bearing the offending mark. 15 U.S.C. § 1125(c)(2).

7. Implications Online. The federal dilution statute provides owners of famous marks with a strong remedy against those who use similar marks or domain names, while potentially placing at risk domain names registered by individuals or businesses in noncompetitive industries that devalue their marks.

C. Internet Domain Names

Domain names identify host computers for email and website addresses. Domain names typically are comprised of an abbreviation, name or acronym, followed by a period and one of five world-wide generic top level domain categories (*.com* for commercial entities, *.edu* for educational institutions, *.org* for non-profit organizations, *.gov* for governmental entities, and *.net*) or country code domains (such as *.ca* for Canada or *.au* for Australia).

The Domain Name System (DNS) provides the mechanism for converting domain names into IP addresses and then back again. The modern domain name system, which was adopted in January 1986, was developed in 1983 by Paul Mockapetris, Craig Partridge and Jon Postel to accommodate increased use, and offered a tree-branch hierarchy of domain names emanating from seven top-level domains (TLDs): *.edu*, *.com*, *.org*, *.gov*, *.mil*, *.net*, *.int* (for international organizations), as well as country domains. Today, the Domain Name System is under the authority of the Internet Assigned Numbers Authority (IANA), which has delegated the operational Internet Registry to InterNIC (the Internet Network Information Center). InterNIC currently administers domain names registered in the *.com*, *.edu*, *.net* and *.org* TLDs. The U.S. Federal Networking Council is responsible for registrations in the *.gov* TLD, and has delegated that authority to InterNIC. Nicholas R. Trio, "What's in a Name?," OnTheInternet, Sept./Oct. 1996, at 20, 21, 22.

Many companies which otherwise are vigilant about protecting their trademark rights did not act quickly in the early 1990's to reserve the domain name equivalents of their trademarks. For example, Sprint initially was allowed to register the *mci.com* domain name. To underscore this point, a Wired magazine editor (Joshua Quittner) registered *mcdonalds.com* and began using the email address *ronald@McDonalds.com*. See Joshua Quittner, "Billions Registered,"

Wired, Oct. 1994; Richard Raysman & Peter Brown, "On-Line Legal Issues," N.Y.L.J., Feb. 15, 1995, at 3.

While two-thirds of the Fortune 500 companies had not registered an obvious version of their trade names as domain names as of October 1994, by 1995 some companies had attempted to register hundreds of potential names. For example, Kraft/ General Foods registered 150 domain names and Proctor & Gamble Co. registered 200, including *badbreath.com*, *dandruff.com*, *diarrhea.com* and *underarm.com*. D. Krivoshik, "Paying Ransom on the Internet," N.J.L.J., Oct. 23, 1995, at 10. It did not take long before serious disputes arose.

1. Common Disputes. Most trademark-related disputes fall into one of four categories, which in turn afford mark owners four primary remedies:

   a. Traditional Cybersquatting, where a third-party has intentionally registered someone's mark – thereby preventing the rightful owner from using it as a domain name – usually for the purpose of profiting by selling it to the trademark owner or otherwise taking commercial advantage of it;

   b. Traffic Diversion Cybersquatting, where a third-party intentionally registers a trademark or (more typically) an obvious derivation, misspelling, pluralization or hyphenated variation of a recognized mark or website address (often pseudonymously) in order to divert traffic to a different location (often a porno site), usually to earn revenue by (a) selling advertisements at that location or (b) referring traffic to a specific site for a fee (but not specifically by selling the domain name to a trademark owner or preventing the owner from using its mark in cyberspace);

   c. Potential Fair Use Cases (referred to derisively by some attorneys for domain name owners with weak or no trademark rights as *reverse domain name hijackings*), were a party has innocently registered a domain name that a trademark owner seeks to acquire; and

   d. Conflicts Between Competing Trademark Owners, where both parties claim rights in the same name.

   Ian C. Ballon, *E-Commerce and Internet Law – A Legal Treatise with Forms* § 11.01 (Glasser LegalWorks 2001).

2. Primary Remedies

   Although domain name disputes may lead to contract, right of publicity or other claims, the overwhelming majority involve trademark disputes, for which rights owners typically have up to four available remedies:

a. Trademark Infringement Litigation (supra § II(A); infra § II(C)(4)), where an owner must establish likelihood of confusion (potentially based only on *initial interest confusion*) between its mark and a third party's domain name (which is shown through a multi-part balancing test);

b. Dilution Litigation (supra § II(B)), if a plaintiff can establish that its mark is "famous" (determined by a multi-part balancing test) – either generally or potentially in a niche market – and that the defendant's use is devaluing the mark (shown by evidence of dilution, tarnishment, blurring, disparagement or diminishment of value), recognizing that there is presently a significant circuit split on the issue of the level of proof required to obtain injunctive relief (making the selection of venue in a dilution case potentially quite important);

c. Litigation under the Anti-Cyberquatting Consumer Protection Act (ACPA) (infra § II(C)(3)), where: (1) a plaintiff need not prove use in commerce (which is otherwise required to bring infringement or dilution claims under the federal Lanham Act) so long as it can show a bad faith intent to profit from use *or registration* (including merely warehousing) *or trafficking* in a domain name; (2) relief may be available for registration of personal names that are not used as trademarks; and (3) *in rem* jurisdiction may be obtained if the domain name registrant has used phony contact information when registering its domain name or otherwise cannot be personally served; or

d. ICANN Arbitration under the UDRP (infra § III(C)(5)), which, like the ACPA, only applies to cybersquatting and may be initiated even where the true identity of a domain name registrant is unknown; but which in theory requires a showing of use, not merely registration or warehousing of a domain name.

e. Filing a UDRP claim may trigger a claim under the Anti-Cybersquatting Consumer Protection Act, but a UDRP ruling is entitled to no deference in litigation. Barcelona.com, Inc. v. Barcelona, 330 F.3d 617 (4th Cir. 2003); see also Hawes v. NSI, 337 F.3d 377 (4th Cir. 2003) (holding that a foreign UDRP proceeding could trigger a claim under the ACCPA); Storey v. Cello Holdings, LLC, 347 F.3d 270 (2d Cir. 2003) (dismissal of an ACCPA suit did not bar a subsequent UDRP action or a later ACCPA action; the UDRP was structured to allow "two bites at the apple").

3. The Anticybersquatting Consumer Protection Act

a. Bad faith registration, trafficking or use of a domain name. The statute affords a private cause of action to the owner of a mark (including a personal name protected as a mark) if, *without regard to the goods or services of the parties,* a defendant (1) has a bad faith intent to profit from the mark; and (2) "registers, traffics in, or uses" a domain name that is:

- "identical or confusingly similar" to a mark that was distinctive at the time the domain name was registered;
- "identical or confusingly similar" to a mark that was famous at the time the domain name was registered; or
- is a "trademark, word or name" protected by 18 U.S.C. § 706 or 36 U.S.C. § 220506.

b. Defense. Bad faith may not be found if a court determines that a defendant "believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful." The statute includes a nonexclusive list of factors that may be considered to evaluate whether "bad faith" exists within the meaning of the statute. Among other things, courts may consider –

- the trademark or other intellectual property rights of the person, if any, in the domain name;
- the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;
- the person's prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
- the person's bona fide noncommercial or fair use of the mark in a site accessible under the domain name;
- the person's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the good will represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation or endorsement of the site;

- the person's offer to transfer, sell, or otherwise assign the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person's prior conduct indicating a pattern of such conduct;

- the person's provision of material and misleading false contact information when applying for the registration of the domain name, the person's intentional failure to maintain accurate contact information, or the person's prior conduct indicating a pattern of such conduct;

- the person's registration or acquisition of multiple domain names which the person knows are identical or confusingly similar to marks of others that are distinctive at the time of registration of such domain names, or dilutive of famous marks of others that are famous at the time of registration of such domain names, without regard to the goods or services of the parties;

- the extent to which the mark incorporated in the person's domain name registration is or is not distinctive and famous within the meaning of 15 U.S.C. § 1125(c)(1).

15 U.S.C. § 1255(d)(1)(B)(i); see also Sporty's Farm L.L.C. v. Sportsman's Market, Inc., 202 F.3d 489 (2d Cir.) (finding bad faith based on other grounds), cert. denied, 530 U.S. 1262 (2000); DaimlerChrysler v. Net Inc., 388 F.3d 201 (6th Cir. 2004) (finding that an inmate and his partner's *foradodge.com* domain name was confusingly similar to plaintiff's *4ADODGE.COM* in violation of the statute); Coca-Cola Co. v. Purdy, 382 F.3d 774 (8th Cir. 2004) (granting injunctive relief against an anti-abortion activist used deceptively similar names with a bad faith intent to profit); Garden of Life, Inc. v. Letzer, 318 F. Supp. 2d 946 (C.D. Cal. 2004) (entering a preliminary injunction ordering the transfer of approximately 75 domain name registrations).

(1) Remedies. Among other remedies, mark owners may obtain an order compelling a defendant to forfeit or transfer a domain name or cancel the registration. Injunctive relief and damages may be recovered on the same terms as otherwise are available under the Lanham Act.

(2) Statutory damages. A plaintiff alternatively may elect special statutory damages of between $1,000 and $100,000 per domain name, set at an amount that "the court considers

just," in lieu of actual damages and profits. This relief may be elected at any time prior to the entry of final judgment, but is only available for bad faith registration claims brought under 15 U.S.C. § 1125(d)(1). See 15 U.S.C. § 1117(d). The remedy of statutory damages – unlike other remedies under the statute – only applies to violations that occur on or after November 29, 1999.

c. *In Rem* Relief. The statute affords mark owners *in rem* relief against the domain name itself if the domain name violates the rights of the owner of a registered mark or a mark protected generally under the Federal Trademark Dilution Act or under section 1125(a) of the Lanham Act and a court expressly finds that the owner either was unable to obtain personal jurisdiction over the defendant or, through due diligence, was unable to find her by (1) sending a notice of the alleged violation and intent to proceed with an *in rem* action under the statute to the postal and email addresses provided by the registrant to a domain name registrar; and (2) publishing a notice of the action "as the court may direct promptly after filing the action." See id. § 1125(d)(2)(A).

(1) Remedies limited. If an *in rem* action is brought, the statute limits a mark owner's remedies to forfeiture or cancellation of the domain name or an order transferring it to the mark owner.

(2) Relief not limited to cybersquatting cases. In Harrods Ltd. v. Sixty Internet Domain Names, 302 F.3d 214 (4th Cir. 2002), the Fourth Circuit ruled that *in rem* actions could be maintained under section 1125(d) based on infringement or dilution, in addition to cybersquatting.

(3) Extra-judicial relief/Registrar Liability. The statute also affords mark owners the opportunity to obtain extra judicial remedies from domain name registrars and registries in cases where *in rem* relief is sought. Specifically, upon receipt merely of "written notification" of a "filed, stamped copy of a complaint filed by the owner of a mark in a United States district court" any domain name registry, registrar or "other domain name authority" is required to: (1) expeditiously deposit with the court documents sufficient to establish the court's control and authority regarding the disposition of the registration and use of the domain name; and (2) "not transfer, suspend, or otherwise modify the domain name during the pendency of the action" except to the extent ordered to do so by the court. Notwithstanding these obligations, domain name registrars,

registries and other domain name authorities are exempted from liability for injunctive relief or damages "except in the case of bad faith or reckless disregard, which includes a willful failure to comply" with a court order.

(4) Constitutionality upheld. The constitutionality of *in rem* relief under ACPA was upheld in CNN L.P. v. cnnnews.com, 162 F. Supp. 2d 484 (E.D. Va. 2001) and Caesar's World, Inc. v. Caesar's - Palace.com, 112 F. Supp. 2d 502 (E.D. Va. 2000). *In rem* jurisdiction may be constitutionally exercised where due diligence is used to effectuate personal service or otherwise provide notice. See, e.g., Alitalia-Linee Italiane S.p.A. v. Casinoalitia.com, 128 F. Supp. 2d 340 (E.D. Va. 2001). *In rem* jurisdiction may not be asserted where personal jurisdiction may be obtained. See id; see also Ford Motor Co. v. Great Domains.com, Inc., 177 F. Supp. 2d 656 (E.D. Mich. 2001); Lucent Technologies, Inc. v. Lucentsucks. com, 95 F. Supp. 2d 528 (E.D. Va. 2000).

(5) Venue limitation. Some courts have held that an *in rem* action under the ACPA must be brought in the jurisdiction where the domain name registry, registrar or other domain name authority is located. See Mattel, Inc. v. Barbie-Club, 310 F.3d 293 (2d Cir. 2002); Fleetbosten Financial Corp. v. Fleetbostonfin.com, 138 F. Supp. 2d 121 (D. Mass. 2001).

d. Protection for the names of individuals. The Act establishes a cause of action against persons who register a domain name that consists of the name of another living person (or a name substantially and confusingly similar) without the person's consent, "with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party . . . ." Liability may not be imposed, however, where a domain name is registered in good faith and "is used in, affiliated with, or related to" a work protected under U.S. copyright law if the registrant is the copyright owner or a licensee, the person intends to sell the domain name in conjunction with the lawful exploitation of the work and the registration is not prohibited by any contract with the named person. The Act does not afford relief for the estates of deceased persons.

(1) Remedies. Courts are authorized to award injunctive relief, including the forfeiture or cancellation of a domain name or its transfer to the plaintiff. Courts also are authorized, in their discretion, to award costs and attorneys' fees, to the prevailing party.

(2) Prospective application. These special remedies only apply to violations that occur on or after November 29, 1999. Individuals, however, also may obtain relief for bad faith registration, trafficking or use of a domain name pursuant to 15 U.S.C. § 1125(d)(1), which affords relief (although not statutory damages) for domain names registered prior to November 29, 1999.

e. Liability limitations for domain name registrars and registries. The Act grants registries, registrars and others a blanket exemption from damages under the statute "for the registration or maintenance of a domain name for another absent a showing of bad faith intent to profit from such registration or maintenance of the domain name." As discussed above, other limitations also are created by the Act.

f. Case law. Case law interpreting the ACPA may be obtained in the update section for chapter 11 at www.ballononecommerce.com.

4. Domain Name Confusion

a. Initial interest confusion

(1) In Interstellar Starship Services, Ltd. v. Epix Inc., 184 F.3d 1107 (9th Cir. 1999), cert. denied, 528 U.S. 1155 (2000), the Ninth Circuit ruled that likelihood of confusion may be established in cyberspace merely based on initial confusion (even if such confusion may be clarified once a visitor reaches an unintended site). See also Brookfield Communications, Inc. v. West Coast Entertainment, 174 F.3d 1036 (9th Cir. 1999); New York State Society of Certified Public Accountants v. Eric Louis Associates, Inc., 79 F. Supp. 2d 331 (S.D.N.Y. 1999). In a subsequent decision in the *epix.com* case, the Ninth Circuit affirmed the district court's order enjoining defendants from making infringing uses of the domain name, but allowing the defendant to retain the domain name and finding that defendants' use did not cause initial interest confusion, dilute plaintiff's mark or constitute cybersquatting. See Interstellar Starship Services, Ltd. v. Epix Inc., 304 F.3d 936 (9th Cir. 2002).

(2) The doctrine of initial interest confusion has not been universally recognized. In Checkpoint Systems, Inc. v. Check Point Softwaretechnologies, Inc., 269 F.3d 270 (3d Cir. 2001), for example, the Third Circuit acknowledged

the viability of the doctrine, but recognized it on much narrower terms than in the Ninth Circuit.

(3) In The Nashville Network v. CBS, Inc., Case No. CV 98-1349 NM (ANx), 2000 U. S. Dist. LEXIS 4751 (C.D. Cal. Jan. 16, 2000), Judge Norma Manella ruled that initial interest confusion had to be evaluated by a "reasonably prudent consumer" standard, which could not be established in the case of *tnn.com* where the mark and domain name owners were not competitors. In this case, the court found significant the fact that the mark owner knew about the domain name registration several years before it initiated litigation.

b. In Data Concepts, Inc. v. Digital Consulting, Inc., 150 F.3d 620 (6th Cir. 1998), the Sixth Circuit reversed an order granting summary judgment where the district court failed to consider the number of other websites using "DCI" in their domain names in evaluating likelihood of confusion.

c. No likelihood of confusion was found in Hasbro, Inc. v. Clue Computing, Inc., 66 F. Supp. 2d 117 (D. Mass. 1999), aff'd, 232 F.3d 1 (1st Cir. 2000), where the defendant used *clue.com* as the domain name for an ISP service and there was no suggestion that it chose the name in order to trade on plaintiff's mark (used in connection with a children's board game).

d. Case-sensitive domain names. In CD Solutions, Inc. v. Tooker, 15 F. Supp. 2d 986 (D. Ore. 1998), the owner of mark "CDS" (Commercial Documentation Services) was not permitted to expand the scope of its mark to incorporate *cds.com*, which was used by the defendant to sell CD-ROMs.

5. ICANN's uniform domain name dispute resolution policy (UDRP)**.** On October 24, 1999, ICANN approved its first Uniform Domain Name Dispute Resolution Policy, which may provide quick and inexpensive (albeit uncertain) relief in cases involving cybersquatting than litigation. A copy of the policy may be obtained at <http://www.icann.org/udrp/udrp-policy-24oct99.htm>. As assessment of ICANN arbitration, based on the first 3,400 cases adjudicated, may be found at <www.ballononecommerce.com>.

a. Elements. Rule 3 of ICANN's procedural rules requires complainants to describe (1) the manner in which challenged domain names are identical or confusing; (2) why the domain name registrant (or "Respondent") should be considered "as having no rights or legitimate interest in the domain name(s)"; and

(3) why the domain names should be considered as having been registered and used in bad faith.

b. Bad faith. Bad faith potentially may be shown by any means, including by evidence that a registrant has offered to transfer a domain name to the trademark owner for more than its initial registration fee or for an unspecified price or listed it with a domain name broker shortly after registration. Paragraph 4 of the UDRP provides that the following circumstances – "in particular but without limitation" – evidence bad faith registration and use:

- registration or acquisition "primarily for the purpose of selling, renting, or otherwise transferring the domain name to the complainant . . . or to a competitor . . . for consideration in excess of . . . documented out-of-pocket costs . . . ;"

- registration "in order to prevent the [mark] owner . . . from reflecting the mark in a corresponding domain name" but only where the registrant has "engaged in a pattern of such conduct . . . ;"

- registration "primarily for the purpose of disrupting the business of a competitor . . .;" or

- intentionally attempting to attract Internet users to an online location "for commercial gain" by creating likelihood of confusion between the complainant's mark and the respondent's domain name registration.

c. Use. In some cases – such as where a registrant has merely registered and warehoused a domain name – use may be more difficult to establish. Some arbitrators have found "use" when a registration is obtained for resale (regardless of whether the name is actually attached to a website) or used to display pornography.

(i) In Telstra Corp. v. Nuclear Marshmellows, Case No. D2000-0003 (WIPO Feb. 18, 2000), an Australian arbitrator even found that a registrant was using a domain name that had not been activated because: (1) the registrant had provided phony contact information (a non-existent P.O. box in Australia); (2) the arbitrator found it "inconceivable" that he was not aware of the complainant's trademark rights; and (3) the registrant could not have had any possible legitimate reason to register the name (telstra.org – the name of the largest company listed on the Australian stock exchange). A similar finding was made by an NAF panel in a dispute between a South Carolina

registrant and the largest newspaper in that state. See The State-Record Co. v. Godpilot, Claim No. FA0102000096686 (NAF Apr. 4, 2001) ("We find that Respondent, who lists his registration address in South Carolina, could not have been unaware of this famous mark and its association with Complainant's newspaper.").

(ii) Where use may be difficult to establish, the ACPA – which merely requires use *or* registration *or* trafficking in a domain name – may provide more certain relief (at least in cases where jurisdiction may be obtained in a U.S. court).

d. General principles. ICANN panels apply general principles, rather than the law of any given forum. Cases therefore sometimes are decided differently than they would be in a U.S. court of law. This occasionally leads to anomalous results. Examples of these type of cases may be found at www.ballononecommerce.com.

6. Cybersquatting. A cybersquatter is an individual who intentionally registers a third party's trademark as a domain name in order to extract a payment from the trademark owner or prevent its use of the mark as a domain name. In cybersquatting cases, plaintiffs may elect to proceed with UDRP arbitration or litigation under the ACPA. Other claims – including trademark infringement and dilution – may be joined in litigation. Indeed, even before the passage of the ACPA, relief was available in cybersquatting cases based on trademark infringement and dilution:

a. In Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316 (9th Cir. 1998), the Ninth Circuit affirmed a lower court ruling entering summary judgment in favor of a trademark owner against cybersquatter Dennis Toeppen based on federal and state dilution claims.

b. In Avery Dennison Corp. v. Sumpton, 189 F.3d 868 (9th Cir. 1999), the Ninth Circuit rejected the district court's holding that defendants – who registered over 12,000 surnames as domain names (including *avery.net* and *dennison.net*), which they used to operate a business licensing "vanity" email addresses – were cybersquatters.

c. In Garden of Life, Inc. v. Letzer, 318 F. Supp. 2d 946 (C.D. Cal. 2004), the court ordered approximately 75 domain name registrations transferred from a cybersquatter as part of a preliminary injunction.

7. Misspellings and typographical errors. Beginning in about 1997, cybersquatters began registering obvious typographical errors and common misspellings of recognized trademarks as domain names in order to divert traffic to alternative sites. Traffic diversion cybersquatting is actionable under both the ACPA and ICANN arbitration, as well as under the Lanham Act.

   a. PaineWebber, Inc. v. wwwpainewebber.com, No. 99-0456-A (E.D. Va. Apr. 1999) is a typical traffic diversion case, where injunctive relief was entered against the owners of *wwwpainewebber.com* (with no period between "www" and "painewebber.com").

   b. Many registrants provide phony contact information when they register domain names, making it difficult to track them down. Columbia Insurance Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999) is a case that discusses this problem and a plaintiff's need in such cases to subpoena customer information. For an analysis of how to compel the disclosure of pseudonymous actors, see Ian C. Ballon, *E-commerce and Internet Law – A Legal Treatise with Forms* §§ 56.06, 62.03 (Glasser LegalWorks 2001). A plaintiff's ability to obtain *in rem* relief may obviate the need to compel the disclosure of the identity of a traffic-diversion cybersquatter to obtain relief.

   c. In Shields v. Zuccarini, 254 F.3d 476 (3d Cir. 2001), the Third Circuit affirmed the applicability of the ACPA to a case where the defendant intentionally registered five spelling variations of the plaintiff's domain name. The court affirmed entry of summary judgment, a permanent injunction and awards of statutory damages and attorneys' fees despite Zuccarini's objection that he had changed the sites linked to the five domain names to "political protester" sites after the lawsuit arose.

   d. FTC action. Zuccarini registered more than 5,500 misspellings of third party marks as domain names, many of which were linked to porno and other sites that employed mousetraps – or a succession of pop-up boxes that force a user to review and close multiple advertisements. The FTC filed suit against Zuccarini in 2001 and in May 2002 obtained a court order permanently barring him from diverting or obstructing consumers on the Internet and from launching websites or pages that belong to unrelated third parties. He was also ordered to disgorge more than $1.8 million in ill-gotten profits. See FTC Press Release, "Court Shuts Down Cyberscam Permanently," May 24, 2002.

   e. Challenging pseudonymity. Where the identity of a cybersquatter is not known and *in rem* relief is unavailable, a plaintiff may need

to initiate satellite litigation to compel disclosure of the person's true identity. See infra § VIII(G).

8. Use in commerce

In order to maintain a claim for infringement or dilution, a plaintiff must establish use of a mark in connection with the sale of goods or services in commerce (or a "commercial use in commerce" under the Dilution Act).

a. Cybersquatting – or the practice of registering a third party's trademark as a domain name to prevent the mark owner's use and/or sell it to the trademark owner – has been recognized as commercial use. See Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316 (9th Cir. 1998) (sale or arbitrage); New York State Society of Certified Public Accountants v. Eric Louis Associates, Inc., 79 F. Supp. 2d 331 (S.D.N.Y. 1999) (traffic diversion).

b. In Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036 (9th Cir. 1999), the Ninth Circuit ruled that merely using a domain name as an email address did not constitute the use of a mark in connection with the sale of goods or services, at least under the facts of that case.

c. In Planned Parenthood Federation of America, Inc. v. Bucci, 97 Civ. 0629 (KMW) (S.D.N.Y. Preliminary Injunction entered Mar. 19, 1997), aff'd mem., 152 F.3d 920 (2d Cir.), cert. denied, 525 U.S. 834 (1998), Judge Kimba Wood ruled that the defendant, a pro-life activist who was using the domain name *plannedparenthood.com* for a website on which he posted anti-abortion material, was using plaintiff's mark "in commerce," within the meaning of 15 U.S.C. §§ 1114 and 1125(a), and as a "commercial use in commerce" within the meaning of 15 U.S.C. § 1125(c). The court concluded that even though the defendant did not seek to earn any revenue from the website, he posted materials about a book entitled "The Cost of Abortion" there to help promote sales by the book's author. In addition, the court found significant the fact that defendant's website was part of an effort to promote a business he operated called "Catholic Radio," in connection with which he solicited funds and encouraged third parties to join him in abortion protests. Finally, the court concluded that defendant's use was commercial because his actions were designed to, and in fact did, harm plaintiff commercially. See also Jews for Jesus v. Brodsky, 993 F. Supp. 282 (D.N.J. 1998) (ruling for the mark owner on similar facts), aff'd mem., 159 F.3d 1351 (3d Cir. 1998).

d. In HQM, Ltd. v. Hatfield, 71 F. Supp. 2d 500 (D. Md. 1999), the court ruled that merely because a domain name is registered in the

.com TLD does not mean it is being used for a commercial purpose.

e. In OBH, Inc. v. Spotlight Magazine, Inc., 86 F. Supp. 2d 176 (W.D.N.Y. 2000), the court found that the defendant's use of *thebuffalonews.com* domain name for a parody site constituted a use in commerce because the site included links to defendant's other sites.

f. Under the ACPA, use *or* registration *or* trafficking in a domain name will be sufficient to state a claim.

9. Registrars' duties to trademark owners. See supra § II(A)(5).

10. *In rem* actions to recover domain names. Trademark owners hampered in their ability to locate and sue multiple, pseudonymous or overseas registrants, have attempted to bring *in rem* actions seeking a declaration of rights with respect to the domain names themselves. Such relief generally may only be obtained under the Anticybersquatting Consumer Protection Act.

a. In Umbro Int'l, Inc. v. 3263851 Canada, Inc., 259 Va. 759, 529 S.E.2d 80 (Va. 2000), the Virginia Supreme Court ruled that a domain name registration is a contract right, not property, and therefore was not subject to garnishment under Virginia law.

b. In Dorer v. Arel, 60 F. Supp. 2d 588 (E.D. Va. 1999), a federal court ruled that a domain name registration is merely a contract right, rather than property subject to attachment or levy.

11. Additional gTLDs. In November 2000, ICANN announced that it would introduce seven new Top Level Domains in or after the second quarter of 2001. Those TLDs, some of which are intended to be limited to specific types of registrants or intended uses, are:

NAME	PURPOSE	
*.aero**	Air transport industry	(www.sita.int)
.biz	Businesses	(www.neulevel.com)
*.coop**	Cooperatives	(www.ncba.org)
.info	Unrestricted use	(www.afilias.com)
*.museum**	Museums	(www.musedoma.org)
.name#	Registration by individuals	(www.theglobalname.org)
.pro#*	Accountants, lawyers, and physicians	(www.registrypro.com)

* Restricted
# Only third-level domain names maybe registered (such as john.smith.name; not smith.name).

12. Property rights in domain names

Although a domain name registration is merely a contract, rather than a property right, the Ninth Circuit held in Kremen v. Cohen, 337 F.3d 1024 (9th Cir. 2003) that domain names are subject to conversion under California state law.

D. Trademark Liability for Spamdexing, Metatag Infringement and White-On-White Text

Tags are HTML instructions in web pages that are not visible to visitors who access a site with a normal browser. Metatags are index words inserted in web pages so that the page will be identified when someone performs a search engine query for the word. In order to give greater prominence to a website when search engine queries are performed, some website developers have inserted the same word multiple times in metatags (such as "ski ski ski ski ski ski" for a ski shop), so that a site may appear higher on a search engine list, or have included words otherwise unrelated to the site (such as the names of celebrities or sexual references) to increase the number of times the site is accessed. A number of suits have been filed over the use of trademarks as metatags in sites owned by third parties. More recently, disputes have also arisen over the practice of placing white text on a white background or black text on a black background or otherwise engaging in acts of spamdexing (or the practice of including words on a website to improve a site's position in response to search engine queries).

1. Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036 (9th Cir. 1999). The Ninth Circuit ruled that the unauthorized use of a trademark in metatags constituted trademark infringement.

2. Playboy Enterprises, Inc. v. Calvin Designer Label, 985 F. Supp. 1220 (N.D. Cal. 1997). Plaintiff, the owner of federally registered trademarks for PLAYBOY and PLAYMATE, sued defendants, who used the domain names playboyxxx.com and playmatelive.com to operate a website which included the names "Playmate Live Magazine" and "Get it all here @Playboy." Defendants were enjoined from using the PLAYBOY and PLAYMATE trademarks as

> Defendants' domain name, directory name, or other such computer address, as the name of Defendants' Web site service, in buried code or metatags on their home page or Web pages, or in connection with the retrieval or data or information or on other goods or services, or in connection with the advertising or promotion of their goods or services.

3. The defendant, a former Playboy Playmate, prevailed in part on her fair use defense in a case involving the use of plaintiff's marks as metatags on her site, in Playboy Enterprises, Inc. v. Welles, 279 F.3d 796 (9th Cir. 2002); see infra § II(H).

E. Key Words and Banner Advertisements

1. A key word is a term used in a search engine query. Many search engines sell the right to have a particular banner advertisement appear when a given key word is entered. For example, an automobile manufacturer might pay to have its advertisement appear whenever the word "car" was included in a query. According to one report, key word sales accounted for up to 25% of the revenue generated by top portal sites in 1998. See Greg Miller & Davan Maharaj, "Banner Ads on the Web Spark A Trademark Battle," L.A. Times, Feb 11, 1999.

2. Some (but not all) portal sites will sell third party trademarks as key words.

3. In Playboy Enterprises, Inc. v. Netscape Communications, Inc., 354 F.3d 1020 (9th Cir. 2004), the Ninth Circuit reversed the lower court's entry of summary judgment against Playboy on its Lanham Act claims against Excite and others where Excite had included two Playboy trademarks as part of a package of more than 400 key words sold to third party advertisers (so that the purchaser's banner advertisements for hard core pornography were displayed whenever users included the trademarks in search requests initiated on defendants' search engines). The district court had relied in large part on the questionable conclusion that the words "playboy" and "playmate" are English language words that do not suggest sponsorship or endorsement by any particular company. The Ninth Circuit found that factual disputes relating to initial interest confusion and dilution precluded the entry of summary judgment.

4. A parallel action brought by Estee Lauder, Inc. against The Fragrance Counter in the Southern District of New York ultimately was settled. See Estee Lauder, Inc. v. The Fragrance Counter, Inc., Case No. 1:99 cv 00382 (S.D.N.Y. complaint filed Jan. 19, 1999).

5. Following *Playboy*, the district court in GEICO v. Google, Inc., 330 F. Supp. 2d 700 (E.D. Va. 2004), denied defendants Google, Inc. and Overture Services, Inc.'s motions to dismiss federal Lanham Act claims for trademark infringement, contributory trademark infringement, vicarious trademark infringement, false representation and dilution arising out of their practice of selling advertisements linked to search terms. In that case, the defendants, in response to user queries for plaintiff's GEICO mark, displayed search results that included "Sponsored Links" by paid advertisers. Judge Brinkema of the Eastern District of Virginia

emphasized that the defendants did not simply display results "using neutral and objective criteria" but displayed sponsored links based on a user's use of the GEICO mark. She further distinguished pop-up ad cases where defendants had prevailed (see infra § II(F)) because GEICO had alleged that Google and Overture were doing more than merely using the GEICO mark in "internal computer coding." The decision, however, merely involved the issue of whether GEICO had pled sufficient facts to defeat a motion to dismiss, and was not an opinion on the merits.

As of late 2004, a similar issue was being addressed in a declaratory relief action filed by Google in the Northern District of California. See Google v. American Blind & Wallpaper Factory, Civil Action No. 5340 (N.D. Cal.). American Blind & Wallpaper Factory was the plaintiff in a parallel suit brought by it against Google in the Southern District of New York.

F. Pop Up Ads

1. Pop up ads that appear in response to a user typing a company's trademark, tradename or website may or may not be actionable, depending on whether traditional elements supporting of a cause of action may be shown in a given case.

2. The first injunction issued prohibiting display overlay advertising was issued in Washingtonpost Newsweek Interactive.com v. The Gator Corp., Civil Action No. 02-909-A (E.D. Va. July 16, 2002). The court relied on copyright and trademark law as the basis for its unreported decision in that case.

3. Various cases brought against Gator Corp. were consolidated by the Multi-District Litigation Panel in In re Gator Corp. Software & Trademark Litig., 2003 U.S. Dist. LEXIS 7729 (M.D.L. May 2, 2003).

4. In Wells Fargo & Co. v. WhenU.com, Inc., 293 F. Supp. 2d 734 (E.D. Mich. 2003), the court denied plaintiffs' motion for preliminary injunction, finding that plaintiffs had not demonstrated a strong likelihood of prevailing on the merits of their trademark and copyright infringement claims and had not shown irreparable injury because they waited nine months before bringing a motion for injunctive relief. In that case, WhenU.com delivered three different types of advertisements via its SaveNow software: (1) a small format pop-up window that typically appeared flush to the bottom right-hand corner of a user's desktop; (2) a larger pop-up window that appeared behind some or all of the browser windows that a consumer was viewing; and (3) a horizontal "panoramic" window that ran along the bottom of a user's screen. Plaintiffs had argued that WhenU.com used its marks (1) to hinder users from accessing plaintiffs' Web sites, (2) by deliberately positioning its pop-up ads in close proximity to plaintiffs' marks and (3) to trigger delivery of its

advertisements. In denying plaintiffs' motion, however, the court held that WhenU.com did not use their marks "in commerce" within the meaning of the Lanham Act. The court wrote that WhenU.com only used plaintiffs' marks in its directory, which consumers typically could not access, to determine which advertisements to deliver to them. The court further considered the juxtaposition of advertisements with plaintiffs' Web sites to be a form of comparative advertising. It further ruled that the inclusion of plaintiffs' marks as URLs in the directory was not a use of the marks in commerce and noted that the marks themselves did not appear on the advertisements displayed to consumers. The court ruled, in the alternative, that there was no likelihood of confusion, based in part on its rejection of survey evidence that it stated did remotely approximate actual market conditions.

With respect to plaintiffs' copyright claims, the *Wells Fargo* court ruled that the presence of an overlapping window merely altered the manner in which an individual's computer displayed content on plaintiffs' Web sites, but did not constitute a derivative work. Id. at 769-71.

5. Similarly, in U-Haul Int'l, Inc. v. WhenU.com, Inc., 279 F. Supp. 2d 723 (E.D. Va. 2003), Judge Gerald Bruce Lee of the Eastern District of Virginia granted summary judgment for the defendants on claims for trademark infringement and dilution, unfair competition and contributory copyright infringement. The court ruled, however, that WhenU.com did not use the plaintiff's marks in commerce, but merely used them for a "pure machine-linking function." Judge Lee found significant the facts that WhenU.com's pop-up ads appeared as separate windows that did not "use" U-Haul's marks and only appeared on the screens of users who had downloaded U-Haul's software program.

   In distinguishing this case in a subsequent lawsuit involving the sale of key words, Judge Brinkema of the same district court emphasized that WhenU.com had allowed advertisers to bid on broad categories of terms that included trademarks, but did not market the trademarks as keywords that could be separately purchased. See GEICO v. Google, Inc., 330 F. Supp. 2d 700 (E.D. Va. 2004).

6. In 1-800 Contacts, Inc. v. WhenU.com, 309 F. Supp. 2d 467 (S.D.N.Y. 2003), by contrast, the court found the plaintiff likely to succeed on its trademark infringement claim based on initial interest confusion, but unlikely to prevail on its claim for copyright infringement. In preliminarily enjoining WhenU.com from using the 1-800 Contacts mark (or similarly confusing terms) as elements in the SaveNow software directory or causing defendant Vision Direct's pop-up advertisements to appear when a computer user "made a specific choice to access or find Plaintiff's website by typing Plaintiff's mark into the URL bar of a web browser or into an Internet search engine . . . ," Judge Batts concluded that

WhenU.com was making "trademark use" of plaintiff's mark in two ways – by using it in the database directory of terms that triggered pop-up advertisements and by displaying advertisements for Vision Direct, a competitor, when a user typed plaintiff's marks. She wrote that "WhenU.com is doing far more than merely 'displaying' Plaintiff's mark. WhenU's advertisements are delivered to a SaveNow user when the user directly accesses Plaintiff's website – thus allowing Defendant Vision Direct to profit from the goodwill and reputation in Plaintiff's website that led the user to access Plaintiff's website in the first place." In so ruling, the court expressly disagreed with the *Wells Fargo* and *U-Haul* courts' analyses.

Judge Batts further found that plaintiffs were likely to prevail in establishing likelihood of confusion based on initial interest confusion, writing that the harm to plaintiff "lies not in the loss of Internet users who are unknowingly whisked away from Plaintiff's website; instead, harm to the Plaintiff from initial interest confusion lies in the possibility that, through the use of pop-up advertisements Defendant Vision Direct 'would gain crucial credibility during the initial phases of a deal.'" Id. at 493 (citing an earlier case). Like other courts, Judge Batts was critical of the methodology of survey evidence presented to show likelihood of confusion. However, she found certain results – that 68% of 490 SaveNow users did not know that the software was running on their computers, that 76% of those who knew it was running were unaware of what it did, and that 59% of SaveNow users believed that pop-up advertisements were placed on the sites on which they appeared by the owners of those sites – were at least suggestive of a likelihood of initial interest confusion. Judge Batts further rejected the argument by WhenU.com that its more recent branding of pop-up ads (with "SaveNow!" and a green dollar sign) and use of a disclaimer "buried in other web pages" were sufficient to alleviate consumer confusion.

7. Claims under the Lanham Act may be bolstered by the Ninth Circuit's 2004 decision in Playboy Enterprises, Inc. v. Netscape Communications, Inc., 354 F.3d 1020 (9th Cir. 2004). See supra § II(E)(3).

8. In Directv, Inc. v. Chin, No. SA-03-CA-0660-RF (W.D. Tex. Aug. 26, 2003), the court ruled that the use of pop up ads did not support a cause of action under the Computer Fraud and Abuse Act.

9. The FTC also is monitoring pop up ads in connection with the use of spyware. In FTC v. Seismic Entertainment Productions, Inc.,Civil No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004) – the first lawsuit filed by the FTC challenging the practice – the FTC obtained injunctive relief in late 2004 against defendants who lured consumers into downloading software without their knowledge that reconfigured their computers to deliver pop up advertisements, which was found to be an

unfair and deceptive practice under the Federal Trade Commission Act. In that case, defendants exploited known vulnerabilities in certain Web browsers to gain access to users' computers without their knowledge when the users accessed certain sites controlled by them. The sites then instructed the browsers to display pop-up advertisements from affiliated sites and used "exploit code" to change the user's homepage, override search functions on the browser and download and install spyware and other programs.

G. Trade Dress Protection for Screen Displays and Website Interfaces

1. In contrast to a trademark, trade dress refers to the "total image of a product" and may include packaging, color combinations and graphics. E.g., International Jensen v. Metrosound U.S.A., 4 F.3d 819, 822 (9th Cir. 1993), citing Vision Sports, Inc. v. Melville Corp., 888 F.2d 609, 613 (9th Cir. 1989).

2. In Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763 (1992), the U.S. Supreme Court upheld the appearance of a Mexican restaurant as a company's trade dress, finding that it was inherently distinctive.

3. In Wal-Mart Stores, Inc. v. Samara Brothers, 529 U.S. 205 (2000), however, the U.S. Supreme Court held that in an action for infringement of an unregistered trade dress, a plaintiff must show that its product design has acquired secondary meaning in order to show it is distinctive.

4. In evaluating whether trade dress protection is available, a court should compare factors such as the design and layout of the product, the graphics used, the background, including white graphics, packaging (including identical text found in both packaging), and similar factors. E.g., Lisa Frank, Inc. v. Impact International, Inc., 799 F. Supp. 980 (D. Ariz. 1992).

5. Functionality. The functionality doctrine will bar trade dress protection for all but the most innovative and creative interfaces. "A product feature is functional if it is essential to the use or purpose of the article or if it affects the cost or quality of the article." Inwood Laboratories, Inc. v. Ives Laboratories, Inc., 456 U.S. 844, 851 n.10 (1982). Stated differently, "a design is legally functional . . . if it is one of a limited number of equally efficient options available to competitors and free competition would be unduly hindered by according the design trademark protection." Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763 (1992). However, elements that are separately functional, and hence unprotectable, may be combined and collectively entitled to trade dress protection. E.g., Interactive Network, Inc. v. NTN Communications, Inc., 875 F. Supp. 1398, 1406 (N.D. Cal. 1995); Lisa Frank, Inc. v. Impact International, Inc., 799 F. Supp. 980, 986 (D. Ariz. 1992).

H. Fair Use (Including Consumer Criticism and First Amendment Issues)

1. Use other than as a mark. Fair use is a defense to a suit for infringement of an incontestable mark if the use is "otherwise than as a mark" or if the mark is used in good faith to describe the goods or services of a party or its geographic origin. 15 U.S.C. § 1115(b)(4); New Kids on the Block v. News America Publishing, Inc., 971 F.2d 302 (9th Cir. 1992) (use of plaintiff's mark by newspapers to invite subscribers to call a 900 number dedicated to the musical group associated with the mark held to be a nominative fair use). Whether a commercial use of a mark is fair will depend upon whether (1) the allegedly infringing good or service is one not readily identifiable without use of the mark, (2) the mark is used only to the extent reasonably necessary to identify the good or service, and (3) the user has not done anything to suggest, in conjunction with use of the mark, sponsorship or endorsement by the trademark holder. E.g., Abdul-Jabbar v. General Motors Corp., 85 F.3d 407, 412 (9th Cir. 1996).

2. Fair uses recognized under 15 U.S.C. § 1125(c)(4) include:

   - Noncommercial use;
   - news reporting or commentary; and
   - fair use (of a famous mark) to identify another entity in comparative commercial advertising or promotion to identify competing goods and services.

3. In Playboy Enterprises, Inc. v. Welles, 7 F. Supp. 2d 1098 (S.D. Cal. 1998), aff'd mem., 162 F.3d 1169 (9th Cir. 1998), the court denied plaintiff's application for a preliminary injunction against the former 1981 Playmate of the Year, in a case alleging trademark infringement and dilution based on her use of the "Playmate of the Year" title on her web page, "PMOY '81" as a watermark in the background of her website and the use of the "Playboy" and "Playmate" marks as metatags. The court found that the defendant used plaintiff's marks truthfully to identify herself and therefore was likely to prevail in her fair use defense. See also Playboy Enterprises, Inc. v. Terri Welles, Inc., 279 F.3d 796 (9th Cir. 2002) (affirming in part summary judgment for the defendant but reversing on the issue of whether her use of "PMOY" constituted infringement or dilution).

4. Consumer criticism. The defendant was found likely to prevail on its fair use defense in Bally Total Fitness Holding Corp. v. Faber, 29 F. Supp. 2d 1161 (C.D. Cal. 1998), which involved a "consumer criticism" site. Among other things, the court ruled that there was not likely to be confusion between plaintiff's genuine site and defendant's "BALLY SUCKS" website. See infra § III(E)(4).

5. Parody

a. In People for the Ethical Treatment of Animals v. Doughney, 263 F.3d 359 (4th Cir. 2001), the Fourth Circuit ruled that the defendant's registration of *peta.org* as a parody site captioned "People Eating Tasty Animals" was not a fair use because it was likely to prevent Internet users from reaching plaintiff's own website.

b. In OBH, Inc. v. Spotlight Magazine, Inc., 86 F. Supp. 2d 176 (W.D.N.Y. 2000), the court found that the defendant's use of *thebuffalonews.com* domain name for a parody site was not a fair use because a fair use parody depends on a lack of consumer confusion (which was not found in this case).

c. For further consideration of parody under the Lanham Act, see Mattel, Inc. v. MCA Records, 296 F.3d 894 (9th Cir. 2002) (involving use of a mark in a parody song).

6. Whether use of a domain name is expressive – in which case it may be entitled to First Amendment protection – or merely serves a source-identifying function (in which case it is not) is analyzed in Name.Space, Inc. v. NSI, 202 F.3d 773 (2d Cir. 2000).

III. THE LAW OF CACHING, LINKING, FRAMING, BOTS AND CONTENT AGGREGATION

A. Caching

1. Definition. Caching is the process of storing data on a computer, and therefore involves the creation of a protectable work under the Copyright Act. MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993), cert. dismissed, 510 U.S. 1033 (1994); Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361, 1378 n.5 (N.D. Cal. 1995).

2. Caching occurs at the server level (called proxy caching), when an on-line provider stores a popular site to facilitate quick linking or a company uses a proxy server for security reasons as part of a firewall. Browsers also "locally" cache, or store recently visited web pages in a computer's RAM. See Eric Schlachter, "Caching on the Internet," The Cyberspace Lawyer, Oct. 1996, at 2.

3. Unauthorized caching may constitute copyright infringement and, if protected trademarks are contained on the cached site, create potential liability for trademark infringement or unfair competition.

B. Hypertext Links

1. Definition. Hyperlinks allow a visitor to a site to easily and quickly connect to another location on the World Wide Web. A hyperlink is created by inserting a URL into HTML code, which then allows visitors to the website to point and click to a particular icon or portion of highlighted text and automatically access the linked site.

2. Linking compared to caching. To a user, there may be no practical difference between pointing and clicking on an icon that will connect to a linked website, and pointing and clicking on an icon that will call up a cached site. Unlike caching, however, linking does not involve the creation of a "copy" within the meaning of the Copyright Act except, arguably, when a viewer accesses a website (which causes a temporary copy of the site to be stored in the viewer's screen memory). A party establishing a link therefore could not be held liable for direct copyright infringement. In theory, a linking party might be subject to contributory or vicarious liability based on the infringing temporary copy created on a visitor's screen memory, although it would be difficult to make out such a claim. Potential defenses would include fair use and implied license.

3. Lanham Act Liability. Linking could create Lanham Act liability if the link created consumer confusion about the origin of a site or was unfair or deceptive. A deceptive content link could subject a party to liability. Most links that are not otherwise unfair – especially site links – would not give rise to a cause of action. Potential defendants might be able to assert fair use defenses available under the Lanham Act.

C. Framing

Frames are a feature which, when used in conjunction with certain browsers, allow visitors to a website to view content from other sites without actually leaving the first page. Depending on how they are structured and the visitor's sophistication, frames arguably may make it difficult to discern content that is linked and run in frames from content that is original to the site. This is especially true because the framing site's URL remains displayed at the top of the screen, even while the other site is displayed. Framing is like linking only with an arguably greater opportunity for consumer confusion.

D. Copyright and Related Cases

1. In-line links. In Kelly v. Arriba Software Corp., 280 F.3d 934 (9th Cir. 2002), the Ninth Circuit ruled that the defendant's practice of making available via in-line links and frames full-size copies of photographs as they had appeared on indexed sites (but with the surrounding text and other web content removed) violated the copyright owner's public display right and did not constitute a fair use. This ruling, however, was

subsequently vacated in Kelly v. Arriba Software Corp., 336 F.3d 811 (9th Cir. 2003). The Ninth Circuit ruled that the practice of merely linking to sites in response to user queries was a fair use. See id.

2. Early case law on links and frames

a. Shetland Times Ltd. v. Wills, Edinburgh, Scotland, Court of Session, Oct. 24, 1996 (Lord Hamilton), the Shetland Times Ltd. brought suit against Zetnews Limited and its managing director, Jonathan Wills, based on the content links established by the defendants to plaintiffs' website for the Shetland Times newspaper. Defendant created content links from its site to stories on plaintiff's website, which created the false impression that visitors were accessing news stories from defendants' newspaper. Although widely cited on the Internet, the case has little legal significance in that it is an unreported decision (which under U.K. law has no precedential value) and turned on an interpretation of U.K. statutory law and was rendered without benefit of "detailed technical information . . . in relation to the electronic mechanisms involved." The court found that the plaintiffs had made a *prima facie* showing that the defendants' use of plaintiff's copyrighted headlines on their website constituted a violation of the of section 7 of the Copyright, Designs and Patent Act of 1988 (for which there is no U.S. corollary). The court rejected the argument, however, that the defendants were also liable for establishing the content link.

b. In Futuredontics, Inc. v. Applied Anagramics, Inc., Appeal No. 97-565711 (9th Cir. July 6, 1998), the Ninth Circuit affirmed a district court ruling denying plaintiff's motion for a preliminary injunction in a case where the plaintiff alleged that the defendant created an unauthorized derivative work by framing plaintiff's website.

c. In Bernstein v. J.C. Penney, Inc., Case No. 98 -2958 R (Ex) (C.D. Cal. granting defendants' motion to dismiss Sept. 29, 1998), celebrity photographer Gary Bernstein filed suit against the J.C. Penney department store and cosmetics company Elizabeth Arden alleging copyright infringement based on a link from a J.C. Penney site created in November 1997 to advertise Passion, an Elizabeth Arden perfume promoted by actress Elizabeth Taylor. A link from a portion of that site (which featured online chat with Elizabeth Taylor) led to a site hosted by Internet Movie Database, which maintained a site containing biographical information on Ms. Taylor. That site, in turn, contained links to several other locations – including a site run by Swedish University Network (SUNET) where unauthorized reproductions of two photographs that Mr. Bernstein had taken of Ms. Taylor were posted. In dismissing

plaintiff's suit, Judge Manuel Real of the Central District of California implicitly ruled that the connection between defendant's site and the infringing photograph was too far removed to be actionable under the Copyright Act.

3. Contributory infringement

a. Injunction granted. In Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc., 75 F. Supp. 2d 1290 (D. Utah 1999), the court entered an injunction prohibiting linking where defendants encouraged visitors to a website – via links – to access infringing content located elsewhere. The case involved more than mere linking, however. Defendants – after being ordered to remove unauthorized copies of plaintiff's protected "Church Handbook of Instructions" from their website – created links to three other locations where infringing copies of the book could be accessed. They also posted emails on their site encouraging visitors to browse the linked locations, print copies of the handbook and email copies to third parties. Although the court concluded that plaintiffs had not shown that defendants contributed to the third party acts of infringement by the owners of the linked sites, it ruled that defendants actively encouraged individual users to infringe plaintiff's copyright by browsing the infringing sites (causing unauthorized temporary copies to be cached in a user's screen RAM) and printing or re-posting unauthorized copies on other websites. A different case would have been presented if the linked content was not infringing or if defendants had not actively encouraged third party acts of infringement.

b. Relief denied. A claim based on contributory copyright infringement was rejected in Ticketmaster Corp. v. Tickets.com, Inc., CV 99-7654 HLH (BQRx), 2000 U.S. Dist. LEXIS 4553 (C.D. Cal. Mar. 27, 2000), aff'd mem., No. 00-56574, 2001 U.S. App. LEXIS 1454 (9th Cir. Jan. 8, 2001) – a case involving content (or "deep") linking – in which the court ruled in part that Ticketmaster's purported license restrictions prohibiting this practice were unenforceable because they were contained in Terms and Conditions which users were not actually required to review in order to access the Ticketmaster site. But see Ticketmaster Corp. v. Tickets.com, Inc., CV 99-7654 HLH, 2003 U.S. Dist. LEXIS 6348 (C.D. Cal. Mar. 7, 2003) (denying, at a later stage in the case, Ticket.com's summary judgment motion based on the potential enforceability of Ticketmaster's Terms and Conditions).

c. Links to infringing content. Arista Records, Inc. v. MP3Board, Inc., 00 Civ. 4660 (SHS), 2002 U.S. Dist. LEXIS 16165 (S.D.N.Y. Aug. 28, 2002). See supra § I(F)(12).

E. Lanham Act and Related Cases

1. Deep Linking

a. In Ticketmaster Corp. v. Microsoft Corp., Case No. 97-3055 DDP (C.D. Cal. Complaint filed Apr. 28, 1997), Ticketmaster sued Microsoft for dilution, unfair trade under the Lanham Act and California state law, and declaratory relief relating to content links created from Microsoft's Seattle Sidewalk website to locations on Ticketmaster's site, use of Ticketmaster trademarks on the Seattle Sidewalk site, use of links and references to Ticketmaster to sell advertising on Microsoft's own site, and "misdescriptions" of Ticketmaster goods and services on the Seattle Sidewalk site. Microsoft filed a counterclaim seeking a declaration that the practice of linking websites does not violate U.S. law. The case settled in early 1999 with Microsoft agreeing not to provide any content (or "deep") links to Ticketmaster's site.

b. In Ticketmaster Corp. v. Tickets.com, Inc., CV 99-7654 HLH (BQRx), 2000 U.S. Dist. LEXIS 4553 (C.D. Cal. Mar. 27, 2000) aff'd mem., No. 00-56574, 2001 U.S. App. LEXIS 1454 (9th Cir. Jan. 8, 2001), Judge Harry L. Hupp granted the defendant's motion to dismiss, ruling that "deep linking by itself (i.e., without confusion of source) does not necessarily involve unfair competition." In so ruling, the court rejected Ticketmaster's contract and license-based arguments because users of its site were not actually required to review the site's Terms and Conditions. But see Ticketmaster Corp. v. Tickets.com, Inc., CV 99-7654 HLH, 2003 U.S. Dist. LEXIS 6348 (C.D. Cal. Mar. 7, 2003) (denying, at a later stage in the case, Ticket.com's summary judgment motion based on the potential enforceability of Ticketmaster's Terms and Conditions).

2. Framing

a. In The Washington Post Co. v. TotalNews, Inc., Case No. 97 Civ. 1190 (PKL) (S.D.N.Y. Complaint filed Feb. 20, 1997), plaintiffs the Washington Post Co., Time Inc., Cable News Network, Inc., Times Mirror Co. d.b.a. The Los Angeles Times, Dow Jones & Co. and Reuters New Media Inc. brought suit in the Southern District of New York for common law misappropriation; federal trademark dilution; trademark infringement; false designation of origin, false representations and false advertising; trademark infringement and unfair competition under N.Y. Gen. Bus. L. § 368-e; state law dilution, pursuant to N.Y. Gen. Bus. L. § 368-d; deceptive acts and practices under N.Y. Gen. Bus. L. §§ 349-350; and copyright infringement. Defendants were the owners and operators of the

totalnews.com website that ran plaintiff's websites in frames made to appear like different channels on a television set. The frames used by defendants cut off the borders on some of the websites, arguably devaluing the sites' content. Plaintiffs objected that defendants ran their own advertisements on a site dedicated exclusively to running third party news sites in frames. The case settled, with defendants agreeing to link – but not frame – plaintiffs' sites.

b. In Hard Rock Café Int'l Inc. v. Morton, 97 Civ. 9483, 1999 U.S. Dist. LEXIS 8340 (S.D.N.Y. June 1, 1999), the court ruled, in a case involving a trademark license, that the act of framing a website, under the facts of the case before it, was likely to cause consumer confusion. See also Hard Rock Café Int'l (U.S.A.) v. Morton, 97 Civ. 9483 (RPP), 1999 U.S. Dist. LEXIS 13760 (S.D.N.Y. Sept. 9, 1999).

3. In Playboy Enterprises, Inc. v. Universal Tel-A-Talk, Inc., Civil No. 96-6961 (E.D. Pa. June 1, 1998), the court held that an unauthorized link to a website could not form the basis for a counterfeiting claim. In a later opinion, however, the court held that links from defendants' infringing "Playboy's Private Collection" website to Playboy's website evidenced that they adopted the "PLAYBOY" and "BUNNY" marks in an effort to capitalize on plaintiff's marks. See Playboy Enterprises, Inc. v. Universal Tel-A-Talk, Inc., Civil Action No. 96-6961, 1998 U.S. Dist. LEXIS 17282 (E.D. Pa. Nov. 2, 1998) (permanently enjoining defendants from – among other things – "providing a link to Plaintiff's website 'Playboy.com.'").

4. In Bally Total Fitness Holding Corp. v. Faber, 29 F. Supp. 2d 1161 (C.D. Cal. 1998), a health club chain brought suit against an individual who operated a site entitled "Bally Sucks" as – what the court termed – a "consumer product review of Bally's services." The defendant did not use plaintiff's marks as part of the domain name for the site, although he did include them in metatags. At the outset of the lawsuit, the defendant included a link from the "Bally Sucks" site to "Images of Men," a site that he operated under the same domain name (compupix.com) that displayed and sold photos of naked men. This link subsequently was disabled. Among other rulings, the court expressly rejected the notion that an ordinary link to a pornographic site could create tarnishment:

> The essence of the Internet is that sites are connected to facilitate access to information. Including linked sites as grounds for finding commercial use or dilution would extend the statute far beyond its intended purpose of protecting trademark owners from uses that have the effect of "lessening . . . the capacity of a famous mark to identify and distinguish goods or services."

5. A different result obtained in Archdiocese of St. Louis v. Internet Entertainment Group, Inc., 34 F. Supp. 2d 1145 (E.D. Mo. 1999), in which a court in St. Louis enjoined the defendant's operation of the *papalvisit.com* and *papalvisit1999.com* websites which, in addition to publicizing Pope John Paul's visit to St. Louis, included banner advertisements on virtually every page that were linked to adult websites. The sites also included off-color jokes about the Pope and the Catholic church. The court found that defendants' use tarnished (and therefore diluted) the Archdiocese's alleged common law marks in "Papal Visit 1999," "Pastoral Visit," "1999 Papal Visit Official Commemorative Items" and "Papal Visit 1999, St. Louis." The case was decided in part under Missouri's dilution statute, which does not require a showing that a mark is "famous."

6. In OBH, Inc. v. Spotlight Magazine, Inc., 86 F. Supp. 2d 176 (W.D.N.Y. 2000), the court found that the defendant's use of *thebuffalonews.com* domain name for a parody site constituted a use in commerce within the meaning of the Lanham Act because the site included links to defendant's other sites.

7. In Nissan Motor Co. v. Nissan Computer Corp., 89 F. Supp. 2d 1154 (C.D. Cal.), aff'd mem., 246 F.3d 675 (9th Cir. 2000), Judge Dean Pregerson entered a narrow injunction prohibiting the defendant from displaying automobile-related information, advertising or links (including links to automobile-related portions of Internet search engines) on its site. Uri Nissan, the owner of Nissan Computer Corp., had registered *nissan.com* for his business – Nissan Computer Corp. – in the mid-1990s. In the late 1990s, however, he sought to sell the domain name to Nissan Motor Co. and created links to car sites from his website. In enjoining these new uses, the court also ordered the defendant to include disclaimers identifying the owner of the Nissan Computer Corp. site and disclaiming any affiliation with Nissan Motor Co. (and providing the URL for that site). In a later decision, the Ninth Circuit reversed a permanent injunction to the extent that it enjoined the defendant from placing links to non-commercial sites that included disparaging comments about the plaintiff, which the court ruled violated the defendant's First Amendment rights. See Nissan Motor Co. v. Nissan Computer Corp., 378 F.3d 1002 (9th Cir. 2004).

F. Technological Self-Help Links and frames may be effectively disabled in most cases.

G. The Digital Millennium Copyright Act

1. Third party liability for linking to sites that contain infringing content may be limited by complying with the Digital Millennium Copyright Act. See supra § I(G).

2. In Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2002), the Second Circuit affirmed the district court's entry of an injunction, pursuant to the anti-circumvention provisions of the Digital Millennium Copyright Act (DMCA), prohibiting defendants from establishing links from their sites to locations that offered DeCSS (a software application used to circumvent CSS, an encryption program intended to prevent unauthorized copying of motion pictures or other content stored on DVDs). Although significant, the remedies available under section 1201 potentially have narrow application. The anti-circumvention provisions may provide a remedy to compel a site owner to disable links to third party sites that contain cracker tools. Linking, *per se*, however, could not be enjoined under the DMCA. Only links to locations that contain material that violates section 1201 may be enjoined.

H. Content Aggregation/Bots

1. Content aggregators – such as meta-search engines – aggregate material from other websites.

2. In eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000), eBay brought suit against an aggregator which allowed users to search multiple auction sites simultaneously, alleging copyright, Lanham Act and state law theories of recovery. Judge Whyte of the Northern District of California preliminarily enjoined the defendant from repeatedly accessing eBay's website based on a theory of trespass to chattels under California law. The defendant – Bidder's Edge – had accessed eBay's site up to 100,000 times per day, accounting for as much as 1.53% of the total requests received by eBay and as much as 1.10% of the total data it transferred over the Web to copy content on a database, which was frequently updated but not as current as material actually found on eBay's site.

3. In Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004), Judge Leval, over a strong dissent, affirmed the district court's preliminary injunction prohibiting Verio from accessing Register.com's website on multiple, alternative grounds, in a case that substantially extended eBay, Inc. v. Bidder's Edge, Inc.

   Verio had used bots to repeatedly copy from Register.com's website the WHOIS database (which lists the contact information for all domain name registrants in Top Level Domains for which Register.com acts as a registrar). Verio used this information to contact new registrants soliciting their interest in services that it offered in competition with Register.com and its co-brand and private label partners. Verio, however, provided misleading information, potentially leading registrants to believe that the solicitation for services was coming from a business affiliated

with Register.com. This "bad fact" for Verio undoubtedly colored the court's perception in framing its rule of law.

a. Terms of Use. The Second Circuit found that Verio was likely to prevail on its breach of contract claim because the terms of use posted on its homepage conditioned entry to the WHOIS database on a visitor assenting to those terms. The Second Circuit noted that although in many cases Internet users are asked to click on an "I agree" icon to manifest their assent to the terms of a contract, "[i]t is standard contract doctrine that when a benefit is offered subject to stated conditions, and the offeree makes a decision to take the benefit with knowledge of the terms of the offer, the taking constitutes an acceptance of the terms, which accordingly become binding on the offeree."

b. Trespass. The Second Circuit also affirmed the district court's finding that Verio was likely to prevail on its claim for trespass to chattels. Register.com had alleged that, although it had made its website available to the Internet, Verio had used bots to flood its computer system with traffic to retrieve customer information and that as much as 2.3% of Register.com's system resources were diminished by Verio's use of bots. Verio in fact had conceded that its practices occupied some of Register.com's systems capacity. Indeed, evidence showed that "Verio was aware that its robotic queries could slow the response times of the registrars' databases and even overload them" and that it contemplated using IP aliasing to make it more difficult for Register.com to identify (and presumably block) its attempts to access Register.com's servers. The district court had written that "[a]lthough Register.com's evidence of any burden or harm to its computer system caused by successive queries performed by search robots is imprecise, evidence of mere possessory interference is sufficient to demonstrate the quantum of harm necessary to establish a claim for trespass to chattels." The Second Circuit affirmed the lower court's finding, emphasizing that "[w]hile Verio's robots alone would not incapacitate Register's systems, . . . if Verio were permitted to continue to access Register's computers through such robots, it was 'highly probable' that other Internet service providers would devise similar programs to access Register's data, and that the system would be overtaxed and would crash."

c. Lanham Act. The court affirmed but narrowed the scope of the portion of the district court's order that enjoined Verio under the Lanham Act, from using Register.com's marks in connection with its solicitations.

d. Computer Fraud and Abuse Act. District Court Judge Jones had also ruled that Register.com was likely to prevail on its claim that Verio violated the Computer Fraud and Abuse Act by (1) using bots to harvest customer data from the WHOIS database; and (2) using the harvested data in violation of posted terms of use. This issue, however, was not addressed in the Second Circuit's opinion.

4. In EF Cultural Travel BV v. Zefer, 274 F.3d 577 (1st Cir. 2001), the court entered a preliminary injunction under the Computer Fraud and Abuse Act based on evidence that defendant's use of proprietary information went beyond the authorized use of plaintiff's website. See also EF Cultural Travel BV v. Zefer, 318 F.3d 58 (1st Cir. 2003) (enjoining the creator of a web scraping tool from acting in concert with plaintiffs' competitors in using the tool to access information from plaintiff's website).

5. Content aggregation may also raise infringement and privacy concerns. For example, in Storm Impact, Inc. v. Software of the Month Club, 13 F. Supp. 2d 782 (N.D. Ill. 1998), the court ruled that the defendant's practice of aggregating (free) shareware software from the Internet, which it sold as part of CD ROM compilations, constituted copyright infringement in violation of the terms of the plaintiff's shareware license.

6. The requisite level of damages required to show electronic trespass in a case under California law was subsequently clarified by the California Supreme Court in Intel Corp. v. Hamidi, 30 Cal. 4th 1342 (2003).

7. For more information on this emerging area of law, see <www.ballononecommerce.com>.

I. Visual Search Engine Practices. See supra § I(E)(10).

J. Key Word Sales and Banner Advertisements. See supra §§ II(E), II(F).

IV. MISAPPROPRIATION OF TRADE SECRETS IN CYBERSPACE

A. Definition

1. State law. Trade secret protection is available by virtue of state law and therefore varies by jurisdiction. See, e.g., Cal. Civil Code §§ 3426 to 3426.6. One of the best illustrations of this point was provided by the Texas Supreme Court in 1995, when it rejected the law in force in 39 other states and held that, under Texas law, the discovery rule does not apply to extend the statute of limitations period to bring misappropriation of trade secret claims. Computer Associates Int'l v. Altai, Inc., 918 S.W.2d 453 (Tex. 1996).

2. What is a trade secret?

   a. Restatement of Torts. The most common definition of a trade secret is found in the Restatement of Torts § 757: "A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."

   b. California statutory definition. Cal. Civ. Code § 3426.1(d) defines a trade secret as:

      > Information, including a formula, pattern, compilation, program, device, method, technique, or process that: (1) derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

3. Elements of a cause of action

   a. General principles. To state a claim for misappropriation of trade secrets, generally a plaintiff must show that: (1) software or information incorporates a trade secret; (2) plaintiff took reasonable steps to preserve its secrecy; and (3) the defendant misappropriated the secret or used improper means, in breach of a confidential relationship, to acquire the trade secret. E.g., Data General Corp. v. Grumman Systems Support Corp., 36 F.3d 1147, 1165 (1st Cir. 1994).

   b. A California cause of action. Under California law, the following elements must be proven: (1) the information sought to be protected must have independent economic value, actual or potential; (2) that independent economic value must be derived from not being generally known to the public or to other persons who can obtain economic advantage from its disclosure or use; (3) the information must be the subject of efforts that are reasonable under the circumstances to maintain its secrecy; (4) to be misappropriated, (a) a trade secret must be acquired by a person who knows or has reason to know that the trade secret was acquired by improper means (including theft and breach or inducement of breach of a duty to maintain secrecy) or (b) the trade secret must be used or disclosed by a person who knew or had reason to know that his knowledge of the trade secret was derived from a person who used improper means to acquire it or who owed a duty to the plaintiff to maintain its secrecy or (c) if the

trade secret was acquired by accident or mistake, the acquirer knew or had reason to know that information before undergoing a material change of his position. Cal. Civ. Code §§ 3426.1(d)(1), 3426.1(d)(2), 3426.1(b).

B. Secrecy Required

1. Disclosure destroys the secret. The U.S. Supreme Court held that, "upon disclosure, even if inadvertent or accidental, the information ceases to be a trade secret and will no longer be protected." Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475-76 (1974).

2. Modern standard: reasonable protection. Generally, reasonable efforts to protect the secrecy of an alleged trade secret are all that is required. See, e.g., Gates Rubber Co. v. Bando Chemical Industries, Ltd., 9 F.3d 823, 849 (10th Cir. 1993) (Colorado law). A limited disclosure, for a brief period of time, therefore may not necessarily defeat trade secret protection. See id.

3. A company's failure to following its own procedures. Although there are no "hard and fast" rules that companies must follow to protect their trade secrets, it is important that whatever policies are adopted are actually followed. A company's failure to follow its own procedures provides a basis for denying trade secret protection. CVD, Inc. v. Raytheon Co., 769 F.2d 842 (1st Cir. 1985), cert. denied, 475 U.S. 1016 (1986).

C. Trade Secrets Posted over the Internet

Whether trade secret protection will be lost for information that was misappropriated and posted over the Internet should depend in part on how widely the information was disseminated. Simply because information theoretically may be available to millions of people online does not in fact mean that it was widely accessed (or accessed at all) if posted for a brief period of time at an obscure location or on an unpopular BBS. Three cases brought against former members of the Church of Scientology raise intriguing issues about the scope of trade secret protection in Cyberspace.

The Church of Scientology treats certain of its religious documents as trade secrets that it only discloses to advanced members, in a particular order and manner. In each case, former Scientology members posted confidential documents online and suit was brought against the former members and their Internet access providers.

1. In Religious Technologies Center v. Lerma, 897 F. Supp. 260 (E.D. Va. 1995), Judge Brinkema determined that church documents were not entitled to trade secret protection under Virginia law primarily because the documents "escaped into the public domain and onto the Internet." In a

subsequent opinion, Judge Brinkema granted summary judgment in favor of the Washington Post defendants on plaintiffs' misappropriation of trade secret claim based on his finding that the alleged trade secrets had been posted on the Internet on July 31 and August 1, 1995, and had remained available for more than ten days, until after a T.R.O. was entered on August 11, 1995, "where they remained potentially available to the millions of Internet users around the world." Religious Technology Center v. Lerma, 908 F. Supp. 1362 (E.D. Va. 1995). In support of her ruling, Judge Brinkema cited Religious Technology Center v. Netcom On-Line Communication Services, Inc., 923 F. Supp. 1231 (N.D. Cal. 1995) (infra § V(C)(3)), writing that "[a]lthough the person who originally posted a trade secret on the Internet may be liable for trade secret misappropriation, the party who merely down loads Internet information cannot be liable for misappropriation because there is no misconduct involved in interacting with the Internet." 908 F. Supp. at 1368.

2. A similar result was reached in Religious Technology Center v. F.A.C.T.Net, Inc., 901 F. Supp. 1519 (D. Colo. 1995), in which Judge Kane determined that Scientology documents were not entitled to protection under the Colorado Uniform Trade Secrets Act because "[d]espite RTC and the Church's elaborate and ardent measures to maintain the secretary of the Works, they have come into the public domain by numerous means . . . . The evidence also showed portions of the Works have been made available on the Internet . . . with the potential for downloading by countless users."

3. The same result also was reached in Religious Technology Center v. Netcom On-Line Communication Services, Inc., 923 F. Supp. 1231 (N.D. Cal. 1995), which provides the most thorough analysis of the issue. Judge Whyte of the Northern District of California wrote that although the defendant could not rely on his own improper postings to support the argument that Scientology documents were no longer secret, evidence that others put the material into the public domain prevented plaintiff from further enforcing its trade secret rights in those materials. Id. at 1256. Judge Whyte concluded that "[w]hile the Internet has not reached the status where a temporary posting on a newsgroup is akin to publication in a major newspaper or on a television network, those with an interest in using the Church's trade secrets to compete with the Church are likely to look to the ["alt.religion.scientology"] newsgroup [where the documents were posted]. Thus, posting works to the Internet makes them 'generally known' to the relevant people . . ." Id. Judge Whyte noted, however, that:

> The court is troubled by the notion that any Internet user, including those using 'anonymous remailers' to protect their identity, can destroy valuable intellectual property rights by posting them over the Internet, especially given the fact that there is little opportunity to screen postings before they are made. . . . [O]ne of the

> Internet's virtues, that it gives even the poorest individuals the power to publish to millions of readers . . . can also be a detriment to the value of intellectual property rights. The anonymous (or judgment proof) defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation. . . . Although a work posted to an Internet newsgroup remains accessible to the public for only a limited amount of time, once that trade secret has been released into the public domain there is no retrieving it.

Id. (citations and footnotes omitted).

4. In Ford Motor Co. v. Lane, 67 F. Supp. 2d 745 (E.D. Mich. 1999), a court in Michigan refused to enjoin the publisher of *blueoval.com* from releasing plaintiff's trade secrets on his website. The court concluded that Ford's requested preliminary injunction would have amounted to a prior restraint. In point of fact, there was some suggestion in the facts of the case that the publisher was acting in collusion with an employee bound by a confidentiality agreement such that the publication would have been equivalent to a misappropriation. Other courts might have ruled differently on the same facts.

5. By contrast, the California Supreme Court rejected a First Amendment challenge to the UTSA in DVD Copy Control Association, Inc. v. Bunner, 4 Cal. Rptr. 3d 69 (2003).

D. Trade Secrets Transmitted By Email

A former vice president of Borland Int'l and the C.E.O. of Symantec Corp., a direct competitor of Borland, were indicted by a Santa Cruz County, California grand jury for criminal theft of trade secrets based in part on email messages that Eugene Wang, the former Borland executive, allegedly sent to Gordon Eubanks, Symantec's C.E.O., on the day Wang resigned his position at Borland to go to work for Symantec. People v. Eubanks, 47 Cal. App. 4th 158, 48 Cal. Rptr. 2d 778 (1995), vacated, 14 Cal. 4th 580, 59 Cal. Rptr. 2d 200 (1996). The charges against the defendants ultimately were dismissed.

E. Commercially Marketed Software

Software may constitute or incorporate trade secrets. E.g., MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511, 522 (9th Cir. 1993), cert. dismissed, 510 U.S. 1033 (1994); Data General Corp. v. Grumman Systems Support Corp., 36 F.3d 1147, 1165 (1st Cir. 1994); Gates Rubber Co. v. Bando Chemical Industries, Ltd., 9 F.3d 823, 849 (10th Cir. 1993). Even commercially marketed software, when in source code form, may be deemed to constitute or incorporate a trade secret. E.g., Vermont Microsystems, Inc. v. Autodesk, Inc., 88 F.3d 142, 147-51 (2d Cir. 1996).

F. The Inevitable Disclosure Doctrine

The inevitable disclosure doctrine is a judicial doctrine generally associated with a 1995 Seventh Circuit decision, PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995). Where recognized, the doctrine may provide authority under state trade secret law for restraining a former employee from assuming responsibilities for a competitor comparable to those which she previously held, where the nature of her new position is such that, regardless of her intent, she would inevitably (or even inadvertently) use, rely upon or disclose trade secrets belonging to her former employer, in performing her new duties. Alternatively, where a court is not inclined to prevent an employee from working for a competitor, the risk of inevitable disclosure may justify an order screening out the employee from working on specific technologies or business plans. In Internet-related litigation, the doctrine is increasingly cited by companies with new technologies or market plans as a basis for protecting the value of lead-time when an employee knowledgeable about time-sensitive trade secrets departs to work for a competitor.

1. Legal Basis. The inevitable disclosure doctrine arose out of section 2 of the Uniform Trade Secrets Act which authorizes injunctive relief in cases involving "actual or *threatened* misappropriations." The doctrine has served as the basis for injunctive relief in cases where a former employee had signed a noncompetition agreement, although the existence of such an agreement is by no means required. See, e.g., Branson Ultrasonics Corp. v. Stratman, 921 F. Supp 909 (D. Conn. 1996); Ackerman v. Kimball Int'l, 652 N.E.2d 507 (Ind. 1995); La Calhene Inc. v. Spolyar, 938 F. Supp. 523 (W.D. Wisc. 1996). Since restrictive covenants may be independently enforceable under state contract law, the doctrine more commonly is invoked where a defendant did not sign a noncompete contract and relief is premised on the enforcement of a confidentiality agreement. See, e.g., PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995); Southwestern Energy Co. v. Eickenhorst, 955 F. Supp. 1078 (W.D. Ark. 1997); Merck & Co. v. Lyon, 941 F. Supp. 1443 (M.D.N.C. 1996); Doubleclick, Inc. v. Henderson, Index No. 116914/97 (N.Y. Sup. Ct. Nov. 5, 1997); see generally Ian C. Ballon, "The Internet Applications of the Inevitable Disclosure Doctrine," The Cyberspace Lawyer, Feb. 1998.

2. State by State Review. A number of courts have declined to apply the inevitable disclosure doctrine in individual cases, but none has expressly rejected it. See, e.g., Campbell Soup Co. v. Giles, 47 F.3d 467 (1st Cir. 1995) (Massachusetts law); APAC Teleservices, Inc. v. McRae, 985 F. Supp. 852 (N.D. Iowa 1997); Bridgestone/Firestone, Inc. v. Lockhart, 5 F. Supp. 2d 667 (S.D. Ind. 1997); Glaxo Inc. v. Novopharm Ltd., 931 F. Supp. 1280 (E.D.N.C. 1996), aff'd on other grounds, 110 F.3d 1562 (Fed. Cir. 1997). Injunctive relief under, or consistent with, the inevitable disclosure doctrine has been entered by courts pursuant to section 2 of the UTSA in Arkansas, Delaware, Illinois, Indiana, Iowa, North Carolina and

Wisconsin, and in one state, New York, which has not adopted the UTSA. See Southwestern Energy Co. v. Eickenhorst, 955 F. Supp. 1078 (W.D. Ark. 1997); American Totalisator Co. v. Autotote Ltd., Civil Action No. 7268, 1983 Del. Ch. LEXIS 401 (Del. Ch. Aug. 18, 1983); PepsiCo Inc. v. Quaker Oats Co., 54 F.3d 1262 (7th Cir. 1995) (Illinois); Ackerman v. Kimball Int'l, 652 N.E.2d 507 (Ind. 1995); Uncle B's Bakery v. O'Rourke, 920 F. Supp. 1405, 1435, modified, 938 F. Supp. 1450 (N.D. Iowa 1996); Lumex, Inc. v. Highsmith, 919 F. Supp. 624 (E.D.N.Y. 1996); Doubleclick, Inc. v. Henderson, Index No. 116914/97 (N.Y. Sup. Ct. Nov. 5, 1997); Merck & Co. v. Lyon, 941 F. Supp. 1443 (M.D.N.C. 1996); LaCalhene Inc. v. Spolyar, 938 F. Supp. 523 (W.D. Wisc. 1996). Since the UTSA has been adopted by forty states, the inevitable disclosure doctrine is likely to continue to gain favor. See Ian C. Ballon, "The Internet Applications of the Inevitable Disclosure Doctrine," The Cyberspace Lawyer, Feb. 1998. For an analysis of the applicability of the inevitable disclosure doctrine under California law, which generally prohibits enforcement of noncompetition agreements, see Ian C. Ballon, "Inevitable Disclosure Under California Law," Intellectual Properties, Feb. 1998.

3. In Doubleclick, Inc. v. Henderson, Index No. 116914/97 (N.Y. Sup. Ct. Nov. 5, 1997), an Internet advertising firm obtained a preliminary injunction prohibiting two former Doubleclick executives from competing with their ex-employer for a period of six months. The court found that Doubleclick was likely to prevail on claims of breach of the defendants' duty of loyalty, misappropriation of trade secrets and unfair competition based on evidence that the two defendants had openly planned to form a competing Internet advertising agency while still employed by Doubleclick, which undoubtedly colored the court's assessment of the inevitability of defendant's use or disclosure of trade secrets. Important to the court's ruling was its finding that the Internet advertising business is "an extremely competitive one, with a variety of companies using different software and sales techniques to maximize the effectiveness of its clients' advertising." In this context, defendants' work for their own competing agency would have, in the court's view, inevitably resulted in their use of Doubleclick trade secrets because, given their importance to Doubleclick's operations, the court found it "unlikely that they could 'eradicate [Doubleclick's] secrets from [their] mind.'"

4. Internet Applications of the Doctrine. The inevitable disclosure doctrine may be especially important to Internet businesses given the speed with which both web-based technology and business models have been developing, the value of lead-time to the development of both Internet technologies and business models and, in the context of technology-based trade secrets, the possibility that a given new technology may be primarily or exclusively associated with a single employer. Where applicable, the

inevitable disclosure doctrine may provide a remedy where an employee's technical knowledge of his former employer's trade secrets, know-how or technology is so highly specialized, or where the technology is so closely associated with a single inventor or company, that it would be impossible for the employee to work in the same field without inevitably using, relying upon or disclosing his former employer's proprietary secrets. See Ian C. Ballon, *E-Commerce and Internet Law - A Legal Treatise with Forms* § 15.03(4) (Glasser LegalWorks 2001).

V. SOFTWARE AND INTERNET BUSINESS METHOD PATENTS

A. Overview

Unlike copyright and trade secret protection, which generally may be claimed for most original software programs, patent protection is available only for programs that meet the more rigorous requirements of the patent statute (e.g., novelty, utility, nonobviousness). There is often a trade-off between seeking patent protection for a program, and treating it as a trade secret, since the patentable elements of the program must be disclosed in order to obtain a patent (and, in many foreign countries, must be disclosed at the time an application is filed). The law governing patent protection for computer software is somewhat confused. What is apparent, however, is that it has become easier to obtain software-related patents in light of recent Federal Circuit decisions. In addition, PTO guidelines for patent examiners are specifically intended to facilitate the issuance of more software patents. See U.S. Patent & Trademark Office, Examination Guidelines for Computer-related Inventions (Feb. 1996).

B. What is Patentable?

1. Patent protection is available for the invention or discovery of "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof . . . ." 35 U.S.C. § 101.

    a. An invention must be a machine, manufacture, composition of matter or a process, or an improvement to any of these four categories, in order to qualify for patent protection.

    b. The Supreme Court has held that Congress intended that patents be granted for "anything under the sun that is made by man." Id. quoting Diamond v. Chakrabarty, 447 U.S. 303, 309 (1980), quoting S. Rep. No. 1979, 82nd Cong., 2d Sess. 5 (1952); H.R. Rep. No. 1923, 82nd Cong., 2d Sess. 6 (1952).

2. A program that merely makes insubstantial improvements over prior art will not be entitled to patent protection. Specifically, a "patent may not be obtained . . . if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would

have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains." 35 U.S.C. § 103.

C. Computer Software and Internet Business Models

1. The Supreme Court has held that patent protection is not available for "laws of nature, natural phenomena, and abstract ideas." Diamond v. Diehr, 450 U.S. 175, 185 (1981).

2. Mathematical algorithms have been held to be per se unpatentable. See Diamond v. Diehr, 450 U.S. 175, 185 (1981); Gottschalk v. Benson, 409 U.S. 63, 75 (1972). The rationale for this rule, however, has not been clearly stated. In Diehr the Court viewed mathematical algorithms as part of the laws of nature, while in Benson the Court treated them as ideas. In re Alappat, 33 F.3d 1526, 1543 n.19 (Fed. Cir. 1994).

3. In the past, courts applied a two-step protocol known as the Freeman-Walter-Abele test, the first step of which was to determine whether a mathematical algorithm was recited directly or indirectly in the claim and the second step of which was to determine whether the claimed invention as a whole is no more than the algorithm itself. E.g., In Re Schrader, 22 F.3d 290, 292 & n.5 (Fed. Cir. 1994).

4. The Federal Circuit limited the Freeman-Walter-Abele test in State Street Bank & Trust Co. v. Signature Financial Group, Inc., 149 F.3d 1368 (Fed. Cir. 1998) to purely mathematical applications. The court wrote that a claim containing a mathematical formula meets the requirements for patentability when the formula "implements or applies that formula in a structure or process which, when considered as a whole, is performing a function which the patent laws were designed to protect (e.g., transforming or reducing an article to a different state or thing) . . . ." According to the Federal Circuit, "[t]he dispositive inquiry is whether the claim as a whole is directed to statutory subject matter. It is irrelevant that a claim may contain, as part of the whole, subject matter which would not be patentable by itself." Id. at 1375. The test for patentability focuses on its practical utility.

5. State Street Bank & Trust Co. also stands for the proposition that methods for conducting business online are potentially patentable. In that case, the Federal Circuit held patentable a data processing system that allowed an administrator to monitor and record financial information flows (including daily asset allocations, income, expenses and related information) and allowed for several mutual funds to pool their resources. A number of e-commerce patents have issued since the late 1990s.

D. Patent Protection May Be Lost Through Premature Disclosure

1. U.S. patent protection may be lost if:

a. The invention was known or used by others in the United States, or patented or described in a printed publication anywhere in the world, before the applicant's claimed date of invention; or

b. The invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the patent application; or

c. The applicant has abandoned the invention; or

d. The invention was first patented by the applicant in a foreign country more than 12 months before the date of the U.S. application; or

e. The invention was described in an earlier patent; or

f. The applicant was not the actual inventor; or

g. Before the date of the applicant's invention, the invention was made in the United States by someone else who has not abandoned, suppressed or concealed it.

35 U.S.C. § 102.

2. The requirements for obtaining foreign patents may be even stricter than in the United States, and in many countries an invention must be disclosed at the time the application is filed, which can, under certain circumstances, jeopardize U.S. rights.

E. Internet Patent Litigation

For information on Internet-related patent suits, see Ian C. Ballon, *E-Commerce and Internet Law - A Legal Treatise with Forms*, Chapter 12 (Glasser LegalWorks 2001).

VI. LICENSES, CONTRACTS, MUSIC AND VIDEO

A. Software and Information

1. The First Sale Doctrine. Software vendors typically license, rather than sell software, since a licensor can restrict a licensee's use of software under a license while, under the "First Sale Doctrine," the right to restrict subsequent use (subject to certain exceptions) is lost once the product is sold. See 17 U.S.C. § 109(a). To the extent a "license" is really a

disguised sales agreement, however, its restrictive provisions will be deemed unenforceable.

2. Shrink wrap and click-through licenses.

a. Consumer software licenses are analyzed under the U.C.C. and traditional contract principles. See Ohio v. Perry, 83 Ohio St. 3d 41, 697 N.E.2d 624 (1998) (quoting an earlier version of this paper); see also Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997); ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996); Step-Saver Data Systems, Inc. v. Wyse Technology, 939 F.2d 91 (3d Cir. 1991); Arizona Retail Systems, Inc. v. The Software Link, Inc., 831 F. Supp. 759 (D. Ariz. 1993). Today, many consumers obtain software preloaded onto personal computers, or packaged in boxes at retail stores, where the terms of a license are buried in documentation. As software increasingly is marketed over the Internet, the enforceability of consumer license agreements should continue to improve because consumers will be expressly asked to accept the terms of a license as a precondition of their being granted access to software. See Ian C. Ballon, "Tearing Shrinkwrap in Cyberspace," The Cyberspace Lawyer, Aug. 1996, at 2; see also Hotmail Corp. v. Van Money Pie, Inc., 47 U.S.P.Q.2d 1020 (N.D. Cal. 1998) (assuming – without analyzing – the enforceability of a click-through agreement).

b. Unconscionability

(1) In Brower v. Gateway 2000, Inc., 246 A.D.2d 246, 676 N.Y.S.2d 569 (N.Y. Sup. Ct. 1998), an intermediate appellate court in New York held the very same form contract at issue in *Hill v. Gateway 2000, Inc.* unenforceable because unconscionable. The court generally approved of the "cash now, terms later" form of unilateral contract used by Gateway 2000, but ruled that the arbitration clause contained in the agreement was unconscionable under UCC § 2-302 because of the excessive cost associated with I.C.C. arbitration, which the court characterized as "unreasonable" and wrote "surely serves to deter the individual consumer from invoking the process . . . . " The court concluded that the cost of ICC arbitration was prohibitive, particularly given the amount of the typical consumer claim involved. For example, a claim of less than $50,000 required advance fees of $4,000 (more than the cost of most Gateway products), of which the $2,000 registration fee was nonrefundable even if the consumer prevailed at the arbitration. Consumers would

also incur travel expenses disproportionate to the damages sought . . ."

(2) In Comb v. PayPal, Inc., 218 F. Supp. 2d 1185 (N.D. Cal. 2002), Judge Fogel of the Northern District of California ruled that the arbitration provision in PayPal's click-through terms of service was unenforceable based on both procedural and substantive unconscionability under California law.

c. UCITA. In July 1999 the National Conference of Commissioners of Uniform State Laws (NCCUSL) approved the Uniform Computer Information Transactions Act (UCITA; formerly known as proposed UCC Article 2B), which is intended to govern software and information contracts. A copy of the model law may be obtained at <http://www.law.unpenn.edu/bll/ulc/ucita/>.

As of this writing, only Maryland and Virginia had adopted UCITA.

3. Infringement by exceeding the scope of a license. In a true license, a licensor grants a licensee fewer rights than it is granted under patent or copyright law. A licensee who exceeds the scope of its license can be held liable for patent or copyright infringement. E.g., S.O.S., Inc. v. Payday, Inc., 886 F.2d 1081, 1087-89 (9th Cir. 1989).

4. Breach of contract. A licensee who violates the terms of a license also may be sued for breach of contract. As the scope of copyright protection for computer software has narrowed, contract rights may prove increasingly valuable.

5. Website Terms and Conditions.

a. In Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002), the Second Circuit upheld the lower court's decision not to enforce posted terms on a website that were merely accessible via a link because users were not required to affirmatively assent to the terms prior to downloading the software at issue in the suit. The case should not be construed as holding that click-though contracts are unenforceable; merely that some courts will find assent lacking where alleged contract terms are merely posted (or, as in this case, available via a link) on a website.

b. In Ticketmaster Corp. v. Tickets.com, Inc., CV 99-7654 HLH, 2003 U.S. Dist. LEXIS 6348 (C.D. Cal. Mar. 7, 2003), by contrast, the court found Ticketmaster's Terms and Conditions to be enforceable, where the terms were accessible via a prominent link

at the top of Ticketmaster's homepage and the defendant acknowledged that it was aware that Ticketmaster purported to condition third party use of the site on its posted terms.

B. Music and Video Available Over the Internet

1. Music -- In General. The way in which music may be used on a site – and in particular whether merely a composition or a particular pre-existing recording will be used – will determine which type of licenses may be required. To reproduce a pre-existing recorded song over the Internet, licenses must be obtained for both the underlying musical composition and the particular recording used. Permission from the songwriter (or assignee) and/or her publishing company to perform the work typically are obtained from BMI, ASCAP or SEAC, while reproduction or distribution rights usually may be obtained from publishers through the Harry Fox Agency.

a. Webcasting. Webcasting is the act of transmitting audio or video over the Internet (which currently relies on streaming technology) for simultaneous viewing. Many radio and television stations may be accessed live over the Internet using streaming media players. Other streaming audio or video files are simply stored on a website where they may be viewed or heard at any time.

The Digital Millennium Copyright Act (DMCA) creates a new compulsory license for certain Internet-specific music transmissions (and non-exempt simulcasts) whose primary objective is not to "sell, advertise, or promote particular products other than sound recordings, live concerts, or other music-related events," subject to specific limitations on the number of works from the same phonorecord or artist that may be played in a set time period and the requirement that (other than an announcement immediately preceding a recording) advance programming schedules not be made available. To be eligible for the compulsory license, a website owner also must comply with a number of other specific requirements. 17 U.S.C. § 114(d); Robert W. Clarida, "New Rules for Webcasters," Intellectual Property Strategist, Dec. 1998, at 7. Otherwise, a website owner must negotiate a specific license from the rights owner.

b. Downloadable Music/MP3 Files. MP3 (an abbreviation for the MPEG-1 Audio Layer 3 audio compression algorithm) files are highly compressed CD-quality digital audio files that may be downloaded in a reasonable amount of time for later use. In contrast to analog music recordings, digital files may be quickly and easily downloaded and copied (including for unauthorized

purposes) without any material degradation in sound quality from the original.

2. Statutory law

a. AHRA. In October 1998, the Recording Industry Association of America (RIAA) filed suit to prevent Diamond Multimedia Systems from manufacturing or marketing the Rio media player, which is a small, portable device that allows MP3 files to be played. The RIAA alleged that the Rio player did not meet the requirements for digital audio recording devices under the Audio Home Recording Act of 1992 (17 U.S.C. §§ 1001 et seq.) because it did not employ a Serial Copyright Management System (SCMS) that sends, receives, and acts upon information about the generation and copyright status of the files it plays. See id. § 1002(a)(2). In affirming the District Court's denial of a preliminary injunction, the Ninth Circuit ruled that the Rio did not qualify as a "digital audio device" within the meaning of the statute because it did not reproduce, either "directly" or "from a transmission," a "digital music recording." Recording Industry Ass'n of America v. Diamond Multimedia Systems, Inc., 180 F.3d 1072 (9th Cir. 1999).

b. DMCA anti-piracy provisions. Provisions of the Digital Millennium Copyright Act prohibiting circumvention of "a technological measure that effectively controls access" to a protected work, which are set to take effect on October 28, 2000 (See 17 U.S.C. § 1201), and related prohibitions on the sale or distribution of anti-circumvention tools or services which already are in effect, should increase music industry confidence in their ability to curb piracy (although even prior to October 28, 2000, disabling an anti-piracy device could subject a person to liability for contributory copyright infringement).

The DMCA prohibits the manufacture, importation, provision, offer to the public or trafficking in "any technology, product, service, device, component, or part thereof" that

- "is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access" to a protected work;
- "has only limited commercially significant purpose or use other than" circumvention; or
- which is marketed for purposes of circumvention.

See id. § 1201(a)(2). A technological measure "effectively controls access to a work" if, in the ordinary course of its operation, it "requires the application of information or a process or a treatment, with the authority of the copyright owner, to gain access to the work." Id. § 1201(a)(3)(B). Circumvention of a technological measure, in turn, is defined to mean "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without authority of the copyright owner . . . ." Id. § 1201(a)(3)(A). Similar restrictions are imposed on efforts to restrict the protections afforded by a technological measure. See id. § 1201(b).

These anti-circumvention provisions are not intended to alter the standards for third party copyright liability or impose specific design obligations on consumer electronics, telecommunications or computer manufacturers. See id. § 1201(c). Exceptions also are created for nonprofit libraries, archives and educational institutions, for law enforcement, intelligence and other government activities and for certain reverse engineering and encryption research. See id. §§ 1201(d), 1201(e), 1201(f).

3. Case Law.

a. In Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2002), the Second Circuit affirmed the lower court's preliminary injunction against distribution of DeCSS – a software utility intended to allow users to break the Content Scramble System (CSS), which is an encryption-based security and authentication system that requires the use of appropriately configured hardware (such as a DVD player or computer DVD drive) to decrypt, unscramble and playback (but not copy) motion pictures stored on DVD. In so ruling, the court ruled that the DMCA did not violate the defendants' First Amendment rights.

b. The Constitutionality of the DMCA was likewise upheld in a criminal case. See United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002).

c. In RealNetworks, Inc. v. Streambox, Inc., No. C 99-2070P, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000), the court granted in part and denied in part plaintiff's application for a preliminary injunction. RealNetworks, Inc. had alleged that the defendant's distribution and marketing of "Streambox VCR" and Ripper programs – which could be used to bypass anti-circumvention aspects of RealNetworks' streaming files – violated section 1201 of the DMCA. Streambox VCR allowed users to

access and download copies of RealMedia files that otherwise are intended to be streamed over the Internet – but not downloaded. The Streambox Ripper, by contrast, was a file conversion application that allowed RealMedia files to be converted to other formats such as .wav, .rma and MP3. The program also permitted conversion between each of these formats. The court enjoined defendant's distribution of Streambox VCR, but declined to enjoin Ripper, which it found had legitimate purposes and commercially significant uses. In so ruling, the court concluded that the fair use defense under the Copyright Act had no application to claims under section 1201. The court also held that unlike under the Copyright Act, a copyright owner was not automatically entitled to a presumption of irreparable injury under section 1201.

d. In Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004), the court vacated entry of a preliminary injunction in a case where a competitor circumvented the authentication sequence used in connection with Lexmark toner cartridges so that its printer cartridges would be compatible with Lexmark printers.

e. In Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir. 2004), the Federal Circuit affirmed judgment for the defendant in a case alleging illegal circumvention of the copyrighted codes for controlling plaintiff's garage door openers.

f. In 321 Studios v. MGM Studios, Inc., 307 F. Supp. 2d 1085 (N.D. Cal. 2004), the court enjoined the defendant from selling products used to circumvent copy protection mechanisms in DVDs, which the defendant had argued were intended to allow users to make back up copies of genuine DVDs. The court ruled that the defendant's software was primarily designed and produced to circumvent CSS and was marketed to the public for that purpose. See also Paramount Pictures Corp. v. 321 Studios, 69 U.S.P.Q.2d 2023 (S.D.N.Y. 2004) (enjoining the defendant on similar grounds).

C. Limitation on Licenses: Intellectual Property Misuse

1. Copyright misuse. A copyright owner may not prevail in an infringement action if there is an "attempted use of a copyright to violate antitrust laws" or if a "copyright is being used in manner violative of the public policy embodied in the grant of a copyright." Lasercomb America, Inc. v. Reynolds, 911 F.2d 970-78 (4th Cir. 1990); see also Practice Management Information Corp. v. American Medical Association, 121 F.3d 516 (9th Cir. 1997); DSC Communications Corp. v. DGI Technologies, 81 F.3d 597, 601 (5th Cir. 1996) (following Lasercomb). Most other courts that

have considered the copyright misuse doctrine since 1990 have declined to apply it.

2. Patent misuse. The doctrine of patent misuse, by contrast, has long been established in patent law. E.g., United States Gypsum Co. v. National Gypsum Co., 352 U.S. 457, 465 (1957). Patent misuse may be predicated on actual, or merely proposed license terms. See, e.g., Motorola, Inc. v. Kimball Int'l, Inc., 601 F. Supp. 62, 65 (N.D. Ill. 1984).

3. Trademark and domain name misuse. In Juno Online Services, L.P. v. Juno Lighting, Inc., 979 F. Supp. 684 (N.D. Ill. 1997), a court rejected the theory of trademark misuse in a domain name dispute.

4. Trade secrets licenses. To avoid copyright or patent misuse problems, especially in view of the lower level of copyright protection now afforded computer software, software licenses frequently encompass trade secrets as well as other intellectual property rights in software. A software program may be protectable as a trade secret even where copyright or patent protection is unavailable. E.g., Gates Rubber Co. v. Bando Chemical Industries, Ltd., 9 F.3d 823 (10th Cir. 1993).

D. Antitrust

1. The U.S. Department of Justice Antitrust Guidelines may limit certain licensing practices.

2. 1994 Microsoft settlement. In 1994, the U.S. Department of Justice reached agreement with Microsoft on the terms of a consent decree, pursuant to which Microsoft agreed to curb certain software licensing practices, including the practice of charging hardware manufacturers a per-machine royalty (regardless of whether Microsoft's operating system was preloaded onto a given PC). Initially, the district court declined to approve the consent decree. United States v. Microsoft Corp., 159 F.R.D. 318 (D.D.C.), rev'd, 56 F.3d 1448 (D.C. Cir. 1995). Among other concerns, Judge Sporkin found that the decree did not address Microsoft's alleged practice of using "Vaporware" (pre-announcing software before it exists) to freeze out competitors. The Court of Appeals reversed Judge Sporkin, and, on remand, District Court Judge Thomas Penfield Jackson approved the consent decree. Michelle Quinn, "Judge OKs Pact Settling Microsoft Antitrust Case," The San Francisco Chronicle, Aug. 22, 1995, at A-1.

3. United States v. Microsoft, 147 F.3d 935 (D.C. Cir. 1998).

The D.C. Circuit reversed the District Court's entry of a preliminary injunction prohibiting Microsoft from requiring computer manufacturers who license its Windows operating system to also license and preinstall

Microsoft's browser program, Internet Explorer, finding that the government had failed to show a reasonable probability of success on the merits. The suit, originally filed by the Department of Justice in 1997 and subsequently joined by the Attorneys General of 20 states and the District of Columbia, sought to hold Microsoft in contempt for violating the consent decree settling earlier antitrust litigation. In view of the procedural posture of the case – a contempt application to enforce an earlier consent judgment – the outcome turned in large part on contract construction and was affected by the higher burden of proof imposed on a party seeking a contempt sanction than otherwise would have arisen if the Justice Department had simply filed a new action.

a. Majority Opinion. In the majority opinion written by Judge Stephen Williams, the D.C. Circuit found that the lower court had failed to provide adequate notice before entering injunctive relief, had misconstrued the meaning of the relevant provision of the consent decree and had appointed a special master without justification. Between the lines, the majority expressed significant skepticism of the government's allegations of an illegal tie-in between Windows 95 and Internet Explorer, although it did acknowledge that Microsoft's operating system dominance created "an exceptional risk of monopoly."

b. Increasing Returns to Scale and Network Externalities. Perhaps most influential will be the D.C. Circuit's analysis of the unique nature of the software industry, which it wrote was characterized by increasing returns to scale and network externalities.

(1) Increasing returns to scale. According to Judge Williams, "because most of the costs of software lie in the design, marginal production costs are negligible. Production of additional units appears likely to lower average costs indefinitely." Stated more dramatically, Judge Williams wrote that "the average cost curve never turns upward."

(2) Network Externalities. Network externalities may be explained by the fact that "an increase in the number of users of a particular item of software increases the number of other people with whom any user can share work." As a result, "Microsoft's large installed base increases the incentive for independent software vendors to write compatible applications and thereby increases the value of its operating system to consumers."

(3) Limited Guidance. Given the limited nature of its ruling and the record on appeal, Judge Williams did not offer

substantial guidance on how antitrust law should respond to these factors.

c. Judge Wald's Concurrence. Judge Wald, concurring in part and dissenting in part, agreed that the case should be remanded for further consideration but strongly disagreed with the level of deference that the majority concluded should be paid to Microsoft's assertions about its technology, which she characterized as coming close to endorsing "judicial abdication in the face of complexity." Judge Wald instead would have applied a balancing test – evaluating whether the integration of different software products yielded real benefit to consumers (or what she called *synergies*) and evidence that a genuine market existed for the two products when provided separately.

4. In United States v. Microsoft, 253 F.3d 34 (D.C. Cir.), cert. denied, 534 U.S. 952 (2001), the D.C. Circuit ruled that Microsoft had committed a monopolization violation, but vacated the district court order to break up Microsoft and remanded the case for further consideration of whether Microsoft was liable for tying.

5. Intergraph Corp. v. Intel Corp, 195 F.3d 1346 (Fed. Cir. 1999). The Federal Circuit reversed Judge Edwin B. Nelson's entry of a mandatory preliminary injunction which, although phrased in negative terms, essentially compelled Intel Corp. to continue to cooperate with Intergraph Corp. and provide it with information on new products. Intel, the world's largest designer, manufacturer and supplier of high-performance microprocessors (which in 1996 earned 88% of all revenue from microprocessors sold for use in desktop computers, laptops, servers and workstations), was sued by Intergraph, Corp., a workstation manufacturer that abandoned its own proprietary chips in favor of Intel's in the early 1990s, when Intel used an open architecture. Integraph alleged that thereafter, once Intel shifted to treating its chips as proprietary, Intel refused to sell its products to Intergraph. Intergraph alleged that it was "locked in" to Intel's chips, which (together with advance sales and information, which Intel previously had provided to Intergraph and continued to supply to other OEMs) constituted an essential facility.

6. Kesmai Corp. v. America Online, Inc. (E.D. Va. Complaint filed Sept. 29, 1997).

a. Claims. Kesmai Corp., leader in the field of aggregate online massively multiplayer computer games – or video games available online that are intended to be played by thousands of people simultaneously – brought suit against AOL for Sherman Act 2 violations (monopolization, attempt to monopolize, monopoly leveraging), false designation of origin and misappropriation, false

advertising, trademark dilution, fraud, breach of contract, defamation, tortious interference with prospective business relations, tortious interference with prospective economic advantage and injunctive relief to block AOL's proposed acquisition of CompuServe under Section 7 of the Clayton Act, 15 U.S.C. § 18. Plaintiff alleged that the online interactive game industry was projected to earn $130 million in 1997, $100 million of which would be generated through AOL. AOL filed a counterclaim in March 1998 alleging malicious prosecution.

b. Allegations. AOL, the plaintiff alleged, launched its game channel in 1995. Kensai, which entered into an agreement with AOL to provide content on this channel, initially became one of AOL's top content providers accounting for 25% of total game channel usage. In August 1996, however, AOL purchased INN, a multiplayer game aggregator and developer alleged by Kesmai to have inferior technology that prevented AOL from even carrying it on its game channel until June 1997. After AOL changed its rate structure to a flat fee monthly rate of $19.95, Kesmai alleges that AOL threatened and pressured it to enter into a new agreement on less favorable terms, and provided assurances that Kesmai would be provided the same terms and promotional opportunities as INN. Kesmai alleged that AOL pressured it to allow AOL to purchase it and, when Kesmai refused, AOL placed INN – an AOL subsidiary and Kemsai's direct competitor -in charge of managing AOL's relationship with Kesmai, despite its promise not to do so. AOL also allegedly made INN the exclusive "anchor tenant" for its game channel, after first offering to allow Kesmai to be an anchor tenant as well for between $5-$10 million (which plaintiff alleged was a monopoly rent demanded for the privilege of reaching AOL's 8 million subscribers). Kesmai further alleged that AOL converted all active Kesmai games, which previously could be accessed free of charge, into surcharged premium games, while falsely advising customers that Kesmai, not AOL, was responsible for the change. Kesmai also alleged that two weeks after inducing Kesmai to enter into a new agreement, AOL announced that INN's name was being changed to WorldPlay – which would also be the new name for AOL's game channel – and set up a games menu that effectively rebranded plaintiff's games and created the false impression that plaintiff's games were marketed by WorldPlay. AOL also allegedly denied it any further promotions.

As a consequence of the alleged acts, Kesmai alleged a 92% decrease in usage and related injuries from false statements attributing the new pricing structure to Kesmai and a resulting deterioration of its relations with game developers. Kesmai

alleged that AOL also sought to fix prices. Plaintiff alleged that AOL had monopoly power because it was not possible to get enough participants at web-based game sites to make the market for massively multiplayer computer games viable on the web. Plaintiff also noted, as evidence of its monopoly power, even though AOL lost 200,000 customers when it experienced substantial traffic problems after it introduced its flat rate pricing plan, more than half of these customers returned after concluding there was no viable alternative to AOL. Plaintiff defined the relevant markets by product (for the entire country): (1) the sale of online content and Internet access service to customers; (2) the aggregation of online interactive multiplayer games; and (3) the purchase of aggregated games content by online services.

c. Settlement. The case ultimately settled on the eve of trial when court papers that had been kept under seal would otherwise have been publicly disclosed See Dan Godin, "AOL Gaming Fight Goes to Court," C/NET, June 16, 1998, <http://www.news.com/News/Item/0,4,23229,00.html?st.ne.ni.rel>. The settlement provided for the parties to continue to work together through at least February 2001 and allowed Kesmai to continue as a significant aggregator of games for the AOL games channel. Other terms of the settlement were not publicly disclosed. Reuters, "Kesmai and AOL Settle Dispute," July 6, 1998.

7. Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 456 (E.D. Pa. 1996). In a November 1996 decision, junk email company Cyber Promotions was found not likely to prevail on the merits of its claim that AOL monopolized or attempted to monopolize the market for providing advertising material via electronic transmissions to AOL subscribers. Judge Weiner rejected Cyber Promotions' arguments that the ability to advertise to AOL's subscribers over the Internet via email was an "essential facility" and that AOL has "refused to deal" with Cyber Promotions in violation of Section 2 of the Sherman Act. The court declined to adopt Cyber Promotions' definition of the relevant market as "the market for providing direct marketing advertising material via electronic transmission to AOL's subscribers" because Cyber Promotions and AOL are not direct competitors and antitrust law does not forbid a private company such as AOL "from excluding from its system advertisers like Cyber [Promotions] who refuse to pay AOL any fee (as opposed to those advertisers who do pay a fee) for their advertising on AOL's system." Id. at 462, citing Monsanto Co. v. Spray-Rite Service Corp., 465 U.S. 752, 761 (1984). The court noted that AOL was not blocking Cyber Promotions' email messages in order to charge anticompetitive prices, but was merely doing so because Cyber Promotions was bombarding AOL servers with up to 1.9 million advertisements per day without paying for

them. The court found that there were numerous competitive methods for advertisers such as Cyber Promotions to reach AOL subscribers, including over the Internet. Finally, the court wrote that AOL had legitimate business justifications for blocking Cyber Promotions' email including that it had received the numerous complaints from its subscribers and was burdened by millions of email advertisements sent to its servers and the fact that Cyber Promotions refused to pay AOL any fee to carry its email advertisements.

E. B2B Exchanges

The FTC issued an important policy paper in October 2000 generally approving B2B exchanges, which some commentators had feared raised antitrust concerns (because competitors share information through exchanges). A copy of the report may be found online at http://www.ftc.gov/os/2000/10/index.htm#26.

F. Electronic Signatures

Federal law generally validates electronic signatures in cases where manual signatures otherwise would be required. See 15 U.S.C. §§ 7001 *et seq.*; Ian C. Ballon, *E-Commerce and Internal Law – A Legal Treatise with Forms*, § 20.02[2] (Glasser LegalWorks 2001).

VII. SERVICE PROVIDER LIABILITY FOR DEFAMATION AND OTHER TORTS

The scope of tort liability for service providers was defined in a series of First Amendment cases arising primarily in New York state and federal courts, and in 1996 was modified by Congress.

A. Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).

1. Facts: CompuServe was sued for libel, defamation and unfair competition under New York state law based on allegedly libelous statements about plaintiff's database, Skuttlebut, which were posted on Rumorville USA, a publication available on the Journalism Forum of CompuServe. Rumorville was published by Don Fitzpatrick Associates ("DFA"), which had no employment, contractual or other direct relationship with CompuServe. DFA provided Rumorville to the Journalism Forum under a contract with CCI, an independent company that contracted with CompuServe to "manage, review, create, delete, edit and otherwise control the contents of" the Journalism Forum "in accordance with editorial and technical standards and conventions of style as established by CompuServe." The Journalism Forum's contract with DFA obligated DFA to accept total responsibility for the contents of Rumorville. CompuServe had no opportunity to review Rumorville USA's contents before it was uploaded, and received no part of any fees charged users for

access to Rumorville. CompuServe subscribers pay flat monthly and time usage fees, regardless of the information services they use.

2. Holding: Summary judgment was entered in CompuServe's favor on all claims. The court held that CompuServe, as the equivalent of "an electronic, for profit library," was entitled to the same First Amendment protection as a news vendor (and therefore would be subject to liability for infringement only if it knew or had reason to know of the allegedly defamatory statements), rather than a publisher, subject to a lower standard of proof. The court wrote that "CompuServe has no more editorial control over such a publication than does a public library, book store, or newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so." Id. at 140.

3. Vicarious liability. The court rejected plaintiff's contention that CCI or DFA could be considered agents of CompuServe since each of the three entities were independent of one another. The court characterized CompuServe's right under its contract with CCI to remove text from its system for noncompliance with its standards as merely a means of maintaining "control over the results of CCI's independent work." Id. at 143. Similarly, the court determined that contractual provisions calling for CompuServe to provide CCI with training, necessary support and to indemnify CCI from claims resulting from information appearing in the Journalism Forum did not give CompuServe sufficient control over CCI and its management to render CCI an agent of CompuServe. The court further rejected the notion that CompuServe could be vicariously liable for the actions of DFA, since DFA's contract was with CCI.

B. Stratton Oakmont v. Prodigy Services, Inc., Index No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (Nassau County, N.Y. Sup. Ct. May 26, 1995):

1. Facts. An anonymous Prodigy subscriber posted allegedly defamatory messages about the brokerage firm Stratton Oakmont and its president on "Money Talk," a widely read financial bulletin board where members can post statements regarding stocks, investments and other financial matters. Stratton Oakmont and its president sued Prodigy for defamation, seeking $200 million in damages.

2. Prodigy was held to be a "publisher" (and therefore subject to liability for defamation regardless of actual or imputed knowledge).

3. *Cubby* distinguished. The court found that:

   a. Prodigy held itself out as a family-oriented online service that exercised editorial control over the content of messages on its

bulletin boards, thereby expressly differentiating itself from its competitors and likening itself to a newspaper.

b. Prodigy in fact regulated the content on its bulletin boards by (a) promulgating "content guidelines," (b) using software that automatically prescreened all bulletin board postings for offensive language, and (c) using "Board Leaders" to enforce Prodigy's content guidelines.

c. In Cubby, CompuServe had no opportunity to review the contents of the publication at issue before it was uploaded.

4. "Board Leader" an agent of Prodigy. The court held that for the limited purpose of monitoring and editing "Money Talk," the Board Leader was an agent of Prodigy, notwithstanding express language to the contrary in Prodigy's Bulletin Board Leader Agreement, because Board Leaders were required to follow procedures established by Prodigy, which exercised managerial control over the Leaders.

5. Appeal. Prodigy filed a notice of appeal. "Cameo Clips," Entertainment Law & Finance, July 1995, at 2.

6. Settlement/motion for reargument denied.

a. Settlement. In October 1995, a provisional settlement was reached. Stratton Oakmont agreed to support Prodigy's assertion that it is not a publisher and is not liable for the acts of anonymous subscribers. Michelle Quinn, "Online Libel Suit Dropped," The San Francisco Chronicle, Oct. 25, 1995, at B1.

b. December 1995 Opinion. On December 13, 1995, Judge Ain *denied* Prodigy's motion to vacate the court's May 26, 1995 opinion even though Stratton Oakmont supported Prodigy's motion, and the parties' settlement was conditioned on the court vacating its prior decision. Judge Ain reasoned that litigants would be discouraged from settling cases early in litigation if they knew that courts would, as a matter of course, vacate unfavorable rulings when requested to do so as a condition of settlement. In addition, Judge Ain wrote that his prior opinion dealt with a developing area of law [that] has thus far not kept pace with the technology . . . [creating] a real need for some precedents. To simply vacate that precedent on request because these two parties (or this plaintiff) has lost interest or decided that the litigation would be costly or time consuming would remove the only existing New York precedent in this area leaving the law even further behind the technology.

C. The Telecommunications Act of 1996

1. Stratton Oakmont overruled. Section 509 of the Act provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230 (c)(1). Congress intended the provision to overrule Stratton Oakmont v. Prodigy Services, Inc. and any similar decisions that have treated online "providers and users as publishers and speakers of content that is not their own because they have restricted access to objectionable material." Conference Report 104-458, 104th Cong. 2d Sess. 194 (1996). The Act expressly preempts inconsistent state laws, but does not prevent states from enforcing laws consistent with the purpose of the Section. 47 U.S.C. § 230(e)(3).

2. Policy objectives. The purpose of this portion of the Telecommunications Act is to promote the development of the Internet and other interactive computer services and media, preserve the free market for the Internet and online services without state or federal government regulation, encourage the development of technologies that maximize user control over what information is received, remove disincentives for the development and use of blocking and filtering technologies that parents may use to restrict children's access to objectionable or inappropriate online material and ensure the enforcement of federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer. 47 U.S.C. § 230(b).

3. Effect of the law. Section 230 does not completely insulate online services from liability for defamation. By reversing Stratton-Oakmont, subpart (1) codifies a modified version of the Cubby standard under which a service provider (or user) may be held indirectly liable for third party acts of defamation only in instances where it actually knew that material posted online was defamatory and failed to take any action, or in very limited circumstances where it failed to act despite reason to know that material was defamatory (provided that the basis for imputed knowledge is not the provider's acts of monitoring online content). See Ian C. Ballon, "*Zeran v. AOL*: Why the Fourth Circuit Is Wrong," Journal of Internet Law, Mar. 1998, at 6. While subpart (1) essentially codifies Cubby, subpart (2) (as discussed below (infra § VII(D)(2)) immunizes providers who take certain good faith measures consistent with the Act – such as screening online content – from liability based on that conduct, thus also eliminating liability based on imputed knowledge in certain circumstances. See Ian C. Ballon, "Defamation and Preemption Under the Telecommunications Act of 1996: Why the Rule of Zeran v. America Online, Inc. Is Wrong," The Cyberspace Lawyer, July/Aug. 1997, at 6. But see Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997) (holding that section 230 eliminates both republication and distributor liability), cert. denied, 524 U.S. 937 (1998). The cumulative effect of

subsections (1) and (2) is to create broad protection for interactive computer services and users in connection with potential state law claims (other than intellectual property and criminal claims) based on third party content.

D. The Scope of Preemption of State Claims

1. Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997), cert. denied, 524 U.S. 937 (1998).

a. Facts. A pseudonymous AOL subscriber posted plaintiff's name and home phone number on purported advertisements for highly offensive and vulgar t-shirts celebrating the bombing of the Oklahoma City federal building and praising accused bomber Timothy McVeigh. Zeran learned of the posting on April 25, 1995 (the day it appeared) when a reporter called him. Zeran immediately notified AOL, which assured him that the notice would be removed (although AOL, consistent with its stated policy, refused to post a retraction). Zeran was inundated with angry phone calls. Although the notice was deleted by AOL the day after it was posted, on April 26, 1995, a new notice appeared later that same day. Zeran again contacted AOL, which advised him that the new message would be deleted and that AOL was taking steps to terminate the account of the pseudonymous subscriber known only as "Ken ZZ03." Nonetheless, similarly offensive messages continued to be posted through May 1, 1995. To make matters worse, a DJ in Oklahoma City received a copy of the bogus posting, read it on the air, and urged his listeners to call "Ken." Zeran claimed to have received hostile and offensive telephone calls as a result of the posting at the rate of about once every two minutes in late April 1995. Plaintiff, at AOL's suggestion, contacted the FBI, and was placed under protective surveillance by local police. The deluge of threatening calls continued until May 15, 1995, when they subsided to about 15 per day.

b. Zeran's Suit. In April 1996, after the Telecommunications Act was signed into law, Zeran filed suit against AOL for negligence.

c. Holding. The court held that Zeran's claim was preempted because the Telecommunications Act of 1996 preempts state law and immunizes online providers (and others) from liability not only for republication of defamatory statements (as in Stratton Oakmont) but also for distribution of defamatory material. Whether AOL knew or should have known that "Ken ZZ03"'s defamatory statements were posted online therefore was irrelevant. In the Zeran court's view, the Telecommunications Act of 1996 overruled both Stratton Oakmont *and* the rule of law set forth in Cubby.

d. Criticism. For a critique of the Zeran decision, see Ian C. Ballon, "*Zeran v. OAL*: Why the Fourth Circuit Is Wrong," Journal of Internet Law, Mar. 1998, at 6; Ian C. Ballon, "Defamation and Preemption Under the Telecommunications Act of 1996: Why the Rule of Zeran v. America Online, Inc. Is Wrong," The Cyberspace Lawyer, July/Aug. 1997, at 6.

e. Post-*Zeran* case law. More recent case law is summarized in the update to chapter 42 of Ian C. Ballon, *E-Commerce and Internet Law - A Legal Treatise with Forms* (Glasser LegalWorks 2001 & 2003 Cum. Supp.), which may be freely accessed at <www.ballononecommerce.com>.

2. Broad preemption of state claims and remedies. The Good Samaritan exemption contains two separate subparts. 47 U.S.C. § 230(c)(1) provides absolute immunity from republication liability for any provider or user covered by the Act, while Section 230(c)(2) provides broad immunity in any cause of action where liability is sought to be imposed "on account of . . . any action voluntarily taken in good faith to restrict access to or availability of material . . . considered to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable . . . ." Specifically, the Act provides that:

> (1) . . . No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> (2) Civil Liability – No provider or user of an interactive computer service shall be held liable on account of –
>
> > (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

a. Expansive definition of affected parties. The term "Information Content Provider" is defined to mean "any person that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C. § 230(f)(3). The definition of "interactive computer service" is broad enough to encompass any computer network, including an employer's computer network or intranet. 47 U.S.C. § 230(f)(2).

b. Impact. The Act immunizes network providers or users from a broad range of state law claims where a potential defendant undertook "any action voluntarily . . . in good faith to restrict access to or [the] availability of material that the provider or user considers to be . . . harassing, or otherwise objectionable." Subpart 2 of the Good Samaritan provision also potentially immunizes employers from certain claims based on employee use of email if the employer took steps to come within the scope of the exemption.

3. Immunity extends to third party (but not original) content.

a. In Ben Ezra, Weinstein & Co. v. America Online, Inc., 206 F.3d 980 (10th Cir. 2000), the Tenth Circuit affirmed the entry of summary judgment for the defendant in a defamation case based on allegedly inaccurate stock information provided to AOL by third parties. In *dicta,* the court acknowledged that section 230 immunity would not extend to information that a defendant developed or created itself.

b. In Carafano v. Metrosplash.com, 339 F.3d 1119 (9th Cir. 2003), the Ninth Circuit ruled that the exemption applies even where an interactive computer service "lightly" edits content before it is made available online.

c. Web host not a content provider. In Does v. Franco Productions, 99 C 7885, 2000 U.S. Dist. LEXIS 8645 (N.D. Ill. June 22, 2000), the court dismissed a suit against a web host pursuant to section 230(c)(2), concluding that plaintiff's claims revolved around third party content (rather than material actually created by the defendants themselves).

4. Exceptions where liability may be found.

a. In Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003), a case which involved unusual facts, the Ninth Circuit ruled that an interactive computer service may not be insulated from liability if the decision to post material was made under circumstances where a reasonable person would conclude that the information was not submitted for publication.

b. In Barrett v. Rosenthal, 112 Cal. App. 4th 749 (Cal. App. 2003), an intermediate appellate court in California ruled that liability may be imposed where a defendant knew or had reason to know that material was false. The broad holding in this case plainly is inconsistent with the statute and its legislative history. The opinion subsequently was de-published and is pending review by the California Supreme Court.

5. More current case law. More current case law may be found at www.ballononecommerce.com.

E. Tort Liability for Computer Viruses

For a discussion of potential theories, see Vicky H. Robbins, "Vendor Liability for Computer Viruses and Undisclosed Disabling Devices in Software," 10 Computer Lawyer 20 (1993).

VIII. EMAIL AND ELECTRONIC DISCOVERY

A. What Mode of Communication Does Email Replace?

The Florida Supreme Court observed that "email transmissions are quickly becoming a substitute for telephonic and printed communications, as well as a substitute for direct oral communications." In Re: Amendments to Rule of Judicial Administration, 2.051–Public Access to Judicial Records, 651 So. 2d 1185 (Fla. 1995). Because email communications take the place of both oral *and* written communications, can be saved electronically (and therefore potentially accessed by systems operators), printed in hard copy, and easily re-transmitted by recipients, the privacy rights of senders and recipients of email (at least in unencrypted form) are still being defined by courts.

B. When Is Email Private?

1. Email sent from or received on a home computer via America Online. In United States v. Maxwell, 42 M.J. 568 (U.S. Air Force Crim. App. 1995), aff'd in relevant part, 45 M.J. 406 (U.S. Armed Forces Ct. App. Nov. 21, 1996), the U.S. Air Force Court of Criminal Appeals upheld defendant's court martial conviction, but held that the Electronic Communications

Privacy Act (18 U.S.C. §§ 25100 et seq.,) applies to email transmissions, and found that the defendant had an objective expectation of privacy in email messages stored in AOL's computers which he alone could retrieve through the use of his own assigned password, as well as in email transmitted electronically to other AOL subscribers who had individually assigned passwords. The court wrote that, "unlike transmissions by cordless telephone, or calls made to a telephone with six extensions, or telephone calls which may be answered by anyone at the other end of the line, there is virtually no risk that appellant's computer transmissions would be received by anyone other than the intended recipients. . . . In the modern age of communications, society must recognize that such expectations of privacy are reasonable." On the other hand, the court noted in dicta that the defendant "may well have forfeited his right to privacy to any email transmissions that were downloaded to the computer by another subscriber or removed by a private individual from the on-line service."

A subsequent appellate court concluded that the defendant possessed a "reasonable expectation of privacy, albeit a limited one, in the e-mail messages that he sent and/or received on AOL." 45 M.J. at 417. The court noted that "[t]he fact that an unauthorized 'hacker' might intercept an e-mail message does not diminish the legitimate expectation of privacy in any way." Id. at 418. The court's finding also rested on the proposition that AOL email is more private than "similar messages on the Internet" because AOL email is privately stored for retrieval on AOL computers and AOL maintains a strict policy of not reading or disclosing subscriber email, which the court considered to be a form of contractual privacy protection. The court wrote – incorrectly – that Internet email is insecure because it passes through multiple servers. Id. at 416. In fact, pursuant to TCP/IP protocols, email transmitted over the Internet is broken into packets which are hard to intercept and, separately, virtually impossible to decipher.

The court also held that email messages posted in a chat room or "'forwarded' from correspondent to correspondent, lose any semblance of privacy." Id. at 418. This unqualified determination about the privacy of forwarded messages seems extreme.

2. Judicial Email. In In Re: Amendments to Rule of Judicial Administration, 2.051–Public Access to Judicial Records, 651 So. 2d 1185 (Fla. 1995), the Florida Supreme Court analyzed whether email used within the Florida judiciary constituted "official records" which were required to be retained and stored. Recognizing the different modes of communication that email messages can replace, the court determined that official business email transmissions should be treated like other types of official communications received and filed by the judicial branch, while internal email communications, such as those sent by judges to their staffs, would

not be subject to public disclosure. In particular, the court cited as examples of the type of email messages that should not be retained as "official records": proposed drafts of opinions and orders, memoranda concerning pending cases, proposed jury instructions, votes on proposed opinions, and information obtained from online research services, such as WestLaw.

3. U.S. Government and business records

a. U.S. Government Email. Email sent to or received by government agencies is subject to the Federal Records Act and therefore must be saved in hard copy form. Armstrong v. Executive Office of the President, 877 F. Supp. 690 (D.D.C. 1995). Similarly, email messages retained by the Executive Office of the President are "presidential records" subject to the President's Records Act. See American Historical Association v. Peterson, 876 F. Supp. 1300 (D.D.C. 1995).

b. Email may not be a business record

(1) One court has held that email does not qualify as a "business record," and therefore is not admissible as an exception to the hearsay rule under Federal Rule of Evidence 803(6), because "email is far less of a systematic business activity than a monthly inventory printout." Monotype Corp. PLC v. International Typeface Corp., 43 F.3d 443, 450 (9th Cir. 1994). The court left open the possibility that email could be admissible for other purposes.

(2) Express Policy. A different result might be reached if a company has an express policy governing retention and deletion of email messages.

c. Employee email is discoverable. In Star Publishing Co. v. Burchell, 181 Ariz. 432, 891 P.2d 899 (1994), the court upheld a lower court order compelling production of employee email communications. The Pima County Board of Supervisors, in connection with allegations concerning improprieties in the operation of the County Assessor's Office, had subpoenaed the computer backup tapes of the Assessor's Office containing all documents for 1993, including email communications of employees. While the case appears to have turned primarily on the absence of evidence that the specific email communications were privileged, the dissenting Judge noted that "this may indeed be a case where technology has once again outpaced the law."

d. Electronic records are no less subject to disclosure than paper records. In appropriate circumstances, however, the costs of discovery may be shifted to the requesting party. See, e.g., Rowe Entertainment, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421 (S.D.N.Y. 2002).

C. Encryption and Internet Security

1. Encryption

a. Encryption is the process of converting data (stored in digital form as a series of 1s and Os) into an incomprehensible code through use of an algorithm. Encryption increases the security of email messages sent over the Internet.

b. Encryption is not practical unless a recipient can decrypt an encrypted email message.

2. Litigation over encryption export controls: First Amendment rights in software

A number of suits were brought challenging expert controls on encryption producers (which have subsequently been liberalized).

a. Karn v. Department of State, 925 F. Supp. 1 (D.D.C. 1996).

(1) Facts. Plaintiff submitted commodity jurisdiction requests to the U.S. Department of State to obtain a determination whether he could export the book "Applied Cryptography" by Bruce Schneier and a computer disk containing source code that was reprinted in the book. The State Department determined that the book could be freely exported, but not the disk, which was subject to its jurisdiction under the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR). Plaintiff argued that the government's designation of the disk, but not the book containing the same source code, as a defense article subject to export controls, was arbitrary and capricious and an abuse of discretion in violation of the Administrative Procedures Act. Karn also argued that defendants' conduct violated his constitutional rights to free speech under the First Amendment and substantive due process under the Fifth Amendment.

(2) Ruling. The court dismissed plaintiff's challenge to the State Department's designation of plaintiff's disk as a "defense article" because the Arms Export Control Act

precludes judicial review, and granted summary judgment in favor of the government on defendant's First and Fifth Amendment claims based on the finding that the government's regulations were "content neutral" and the issues raised presented a nonjusticiable political question.

b. A different result was reached in Bernstein v. Department of State 974 F. Supp. 1288 (N.D. Cal. 1997), aff'd, 176 F.3d 1132 (9th Cir. 1999). In that case, Daniel Bernstein had unsuccessfully attempted to post his Snuffle encryption system and related documentation on an Internet discussion group called "sci.crypt." Bernstein brought suit, alleging that the government's suppression of his program under the AECA and ITAR violated his free speech right to express his scientific ideas by publishing an academic paper on the system (which includes the program's source code). The trial court had granted the defendant's motion for summary judgment ruling that the government's encryption regulations, insofar as they required licenses for encryption and decryption software, devices and technology, constitute unconstitutional prior restraints under the First Amendment. The Ninth Circuit's opinion in this case ultimately was withdrawn pending *en banc* review.

c. A more recent First Amendment challenge was also decided against the government. See Junger v. Daley, 209 F.3d 481 (6th Cir. 2000).

3. Current export regulations

In late 2000, the U.S. Commerce Department's Bureau of Export Administration (BXA) published a final rule that permits most encryption products to be exported to the European Union, Australia, Japan, New Zealand, Norway, Switzerland, the Czech Republic, Poland and Hungary. The rule mirrors earlier-enacted EU regulations.

U.S. companies may export encryption products to end-users in the affected countries, pursuant to a license exemption, so long as they submit a commodity classification to the BXA before doing so. U.S. exporters need not wait for any sort of approval after submission, however, before shipping their products. Post-export reporting requirements have also been streamlined for certain products with preloaded software or that otherwise incorporate encryption, such as personal computers, laptops, handheld devices, network appliances and short-range wireless technologies.

The latest regulations may be found at <http://www.bxa.doc.gov/Encryption/guidance.htm>

4. Digital signatures. Digital signatures use cryptographic techniques to identify and authenticate the author of a work and verify that the contents of a file have not been altered in transit. A digital signature contains a mathematically unique sequence of digits determined by the work being protected, the particular algorithm used and the key used in generating the signature. For a copy of the 1996 Digital Signature Guidelines prepared by the Information Security Committee of the ABA's Section of Science and Technology, contact the Section at (312) 988-5599 or sciencetech@attmail.com.

5. Steganography. Also known as "digital fingerprinting" or "digital watermarking." Digital information may be encoded with attributes that cannot be disassociated from the file that contains the information. In late 2001, it was reported that the al Qaeda terrorist organization communicated information to different cells via messages encoded on websites using steganography.

6. Security law. Federal health care and financial services statutes impose security requirements on the protection of personal information. In addition, California has adopted a security reporting statute, Cal. Civil Code §§ 1798.29, 1798.82, which requires security breaches to be disclosed in certain circumstances.

D. Email, Client Confidences and the Attorney-Client Privilege

1. Reasonable protection

Canon 4 of the ABA's Model Code of Professional Responsibility obligates attorneys to "preserve the confidences and secrets" of their clients. Reasonable measures, but not absolute security is what is required. Ronald Abramson, "Protecting Privilege in E-mail Systems," Texas Lawyer, Sept. 5, 1994, at 20.

2. Is the use of email reasonable?

a. Interception is unlawful. The interception by unintended recipients of email messages transmitted over public communication lines is unlawful under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 et seq.; United States v. Maxwell, 42 M.J. 568 (U.S. Air Force Crim. App. 1995), aff'd in part, 45 M.J. 406 (U.S. Armed Forces Ct. App. Nov. 21, 1996); see also People v. Stevens, 34 Cal. App. 4th 56, 63, 40 Cal. Rptr. 2d 92, 96 (1995) (summarizing the ECPA's legislative history).

b. Internet security

(1) It is virtually impossible to intercept an email while in transit over the Internet. Pursuant to TCP/IP protocols, information is transmitted over the Internet in packets. A single message may be broken into several different packets, which may be sent over different routes before being reassembled at their destination point. A single packet would be almost impossible to target and virtually unintelligible.

(2) Many of the concerns about the security of email apply to other modern forms of communications. For example, it is easier to tap a telephone line than intercept an email while in transit. Similarly, many lawyers have received misdirected confidential faxes, yet still routinely transmit confidential documents by facsimile.

c. Gateway security. The connection point between a company or law firm's internal network and the Internet must be protected by a firewall to prevent intruders from hacking into a computer network.

d. Internal security employed by lawyers and clients. The reasonableness of a lawyer's use of email for attorney-client communications should depend in large measure on the policies for use, retention and destruction of email implemented by both the law firm and the client. While no one set of procedures is likely to be determinative, companies should adopt policies to ensure that attorney-client communications are treated confidentially. Among issues to consider are: who routinely has access to email? is access determined by a password? could anyone in the company retrieve the message? are confidential communications routinely transmitted outside of the control group?

e. Is encryption required? Given how difficult it is to intercept an email in transit it should generally be viewed as unnecessary to encrypt email communications, although the additional security will provide protection in case a message is misaddressed. If a communication is encrypted while in transit, decrypted and then left in an email box on an unsecured network, forwarded outside of the control group or otherwise inadequately protected, the fact that it was encrypted while in transit will have little effect on whether it remains confidential. Internal use of encryption – or adequate policies – may be more important than encrypting messages sent over the Internet.

3. Case law

a. Disclosure destroys privilege. Once arguably privileged communications are made available over the Internet, they are in the public domain and any claim to privilege may be lost. See Castano v. The American Tobacco Co., 896 F. Supp. 590, 595-96 (E.D. La. 1995) (tobacco industry documents widely disseminated over the Internet; applying California rules of conduct).

b. Inhouse communications. At least one lower court has expressly ruled that inhouse email communications may be protected. In National Employment Insurance Corp. v. Liberty Mutual Ins. Co., No. 93-2528-G (Mass. Sup. Ct. Dec. 21, 1994), a Massachusetts state court judge ruled that email messages sent between a corporation's inhouse counsel and middle and low-level employees were privileged because undertaken for legal, rather than business purposes. In the alternative, Judge Welch ruled that the email messages were immune from discovery as attorney-work product. "Current Developments" in The Computer Lawyer, Jan. 1995, at 29.

4. Ethics Opinions

In early 1999, the ABA Standing Committee on Ethics and Professional Responsibility issued Opinion No. 99-413, which provides that it is generally reasonable for attorneys to communicate with clients by email.

Several states previously had issued ethical opinions warning against using email for attorney-client communications . These early decisions appear to have been made without an appreciation of the difference between the way information is sent over the Internet and the manner by which it is transmitted to analog cellular phones. Increasingly, states are issuing ethical opinions recognizing that it is generally appropriate to communicate with clients by unencrypted email. See, e.g., Illinois Ethics Op. 96-10 (May 16, 1997); North Dakota Op. 97-09 (Sept. 1997); South Carolina Ethics Op. 97-08 (June 1997); Vermont Opinion 97-5; see also Iowa Ethics Op. 97-01 (Sept. 18, 1997) (communications acceptable with written waiver); see generally <http://www.legalethics.com>.

E. An Employer's Right to Monitor Employee Email

Employees typically send and receive personal email messages in much the same way that they may place and receive personal telephone calls while at work. However, unlike telephone calls (unless recorded, which generally is prohibited absent a court order), email communications are stored electronically (unless and until deleted by the recipient) and can be monitored, either intentionally by employers or surreptitiously by co-workers.

1. In Bohach v. Reno, 932 F. Supp. 1232 (D. Nev. 1996), Judge Edward Reed denied plaintiff's application for a preliminary injunction based on alleged violations arising out of the Reno police department's monitoring alphanumeric pager messages which the plaintiffs, who were both police officers, sent each other over the department's "Alphapage" message system. The system was actually a software program that allowed brief alphanumeric messages to be transmitted to visual display pagers. The software was installed in mid-1994, at which time police officers were told that "every Alphapage message is logged on the network" and should not be used for certain types of messages (such as comments about Department policy or remarks that would violate the Department's anti-discrimination policy). Messages were typed on computers, where they were stored on a server even after transmitted via modem to a paging company for transmission by radio broadcast. The Department's computers could be freely accessed; a password or special clearance was not required. The initial phase of this process, according to the court, "is essentially electronic mail – and e-mail messages are, by definition, stored on a routing computer." Id. at 1234. The court held that the officers did not have an objectively reasonable expectation of privacy in these communications and therefore were not likely to prevail on their Fourth Amendment civil rights claim.

2. Smith v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996). A federal district court in Philadelphia, applying Pennsylvania state law, held that an employee who was fired for the contents of an email he transmitted from a company computer, had no cause of action for wrongful termination. The court found that the employee did not have a reasonable expectation of privacy in his email messages, even though the company had assured its employees that their private email communications would be treated confidentially and would not be intercepted, because the plaintiff sent an offending message over the company's email system to his supervisor. Even if the employee had a reasonable expectation of privacy, the court reasoned that a company's need to deter unprofessional and potentially illegal conduct outweighs any countervailing privacy interest, especially since the court determined that a company's interception of employee email is not highly intrusive.

3. California state trial courts that have considered the issue have upheld an employer's right to monitor employee email. Ricardo Sandoval, "E-mail is Next Frontier in Privacy Debate," San Jose Mercury News, Aug. 13, 1995, at E-1; Abdon M. Pallasch, "Company Policies to Monitor E-mail Licking Edge of Electronic Envelope," Chicago Lawyer, Aug. 1995, at 4. For an alternative view of the privacy issues surrounding employee email, see Larry O. Gantt, "An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace," 8 Harv. J.L. & Tech. 346 (1995).

F. Liability for Email Transmissions

1. Employer liability of employee email.

a. In Fraser v. Nationwide Mutual Ins. Co., 352 F.3d 107 (3d Cir. 2004), the Third Circuit held that an insurance company did not violate the Electronic Communications Privacy Act when it accessed an independent agent's email because there was no "intercept" and because the search by the company, as a service provider, was exempt from liability under the statute.

b. While an employer may, under certain circumstances, be held liable for employee email, it may also be able to claim immunity under the Good Samaritan provisions of the Telecommunications Act of 1996 if it took some action to regulate its computer network. Specifically, an employer who actively undertakes to monitor email as part of "any action voluntarily taken in good faith to restrict access to or [the] availability of material that the provider or user considers to be . . . harassing, or otherwise objectionable" may immunize itself from certain torts and other state law claims based on employee use of a company's email system or intranet. 47 U.S.C. § 230(c)(2); see supra § VIII(D).

2. Employee email as evidence of a crime. A former vice president of Borland Int'l and the C.E.O. of Symantec Corp., a direct competitor of Borland, were indicted by a Santa Cruz County, California grand jury for criminal theft of trade secrets based in part on email messages that Eugene Wang, the former Borland executive, allegedly sent to Gordon Eubanks, Symantec's C.E.O., on the day Wang resigned his position at Borland to go to work for Symantec. People v. Eubanks, 38 Cal. App. 4th 114, 44 Cal. Rptr. 2d 846 (1995), vacated, 96 C.D.O.S. 9329 (Cal. Dec. 23, 1996). The Santa Cruz County District Attorney dismissed charges against Eubanks in November 1996, while the case was pending before the California Supreme Court.

G. Challenging Email Anonymity and Pseudonymity

1. Privacy laws generally compel service providers to maintain the confidentiality of certain subscriber information. The identity of a pseudonymous actor, however, generally may be obtained from service providers absent a contrary provision in their stated privacy policies. See, e.g., Jessup-Morgan v. America Online, Inc., 20 F. Supp. 2d 1105 (E.D. Mich. 1998) (dismissing or entering judgment for the defendant on plaintiff's alleged privacy, breach of contract and tort claims (among others) arising out of AOL's disclosure of plaintiff's identity pursuant to a facially valid subpoena in accordance with the provisions of the Electronic Communications Privacy Act). Consumer-oriented services such as

Yahoo! and AOL, however, typically afford subscribers advance notice before complying with a subpoena, allowing individuals to appear through counsel to challenge the disclosure of their identities.

2. Where pre-service discovery is permitted, courts have established standards that are difficult for plaintiffs to meet. See, e.g., Columbia Insurance Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999).

3. The U.S. Supreme Court has recognized a privacy right to anonymity in political speech cases. This right is not absolute, however. See Ian C. Ballon, *E-Commerce and Internet Law - A Legal Treatise with Forms*, §§ 42.02, 56.06, 62.03 (Glasser LegalWorks 2001 & 2003 Supp.).

4. Some courts have held that the standards for obtaining disclosure of the true identity of a pseudonymous actor should be higher when sought from a third party witness. See, e.g., Doe v. 2TheMart.com, Inc, 140 F. Supp. 2d 1088 (W.D. Wash. 2001) (courts should assess (1) was there a good faith basis to issue the subpoena; and (2) is the information sought centrally needed to advance the claim).

5. Anti-SLAPP sanctions of $55,000 were imposed in one case brought to compel the disclosure of the true identity of an Internet speaker in a defamation case. See Global Telemedia Int'l, Inc. v. Doe, 132 F. Supp. 2d 1261 (C.D. Cal. 2001). But see MCSi, Inc. v. Woods, 290 F. Supp. 2d 1030 (N.D. Cal. 2003) (ruling that pseudonymous posts on a competitor's message board were not subject to the anti-SLAPP statute and constituted merely commercial speech).

6. In cases involving alleged acts of copyright infringement, the Digital Millennium Copyright Act authorizes the issuance of subpoenas to service providers to compel the disclosure of the identity of alleged infringers. However, in RIAA v. Verizon Internet Services, 351 F.3d 1229 (D.C. Cir. 2003), the D.C. Circuit granted Verizon's motion to quash a DMCA subpoena (served to identify pseudonymous alleged infringers), finding that section 512(h) did not authorize the issuance of a subpoena to a service provider acting solely as a conduit for communications not actually stored on its own servers.

H. Spoliation of Evidence

Companies should adopt adequate email, intranet, extranet and electronic communication policies to avoid liability for spoliation of email evidence in the event of litigation. See Ian C. Ballon, "Spoliation of E-mail Evidence: Proposed Intranet Policies and A Framework For Analysis" *The Cyberspace Lawyer*, Mar. 1999; Ian C. Ballon, "How Companies Can Reduce The Costs and Risks Associated With Electronic Discovery," *The Computer Lawyer*, July 1998.

IX. SPAMMING AND THE LAW OF JUNK EMAIL

A. Definition

Spamming, or the practice of disseminating multiple unsolicited copies of junk email over the Internet, may violate the federal CAN SPAM Act and support causes of action by service providers and others based on trademark, trespass and other federal and state laws.

Some mass email distributors use pseudonymous — or false — return email addresses (and phony headers), so that their identity cannot be traced. When someone deliberately assumes a third party's identity, the practice is referred to as *spoofing*.

By masking the true source of a junk email transmission, spammers increase the likelihood that a message will be opened and read, rather than automatically deleted by recipients. Spammers also avoid the burdens associated with complaints and email bombs that are routinely sent by recipients of junk email (by return message).

By using false return email addresses, commercial bulk email distributors impose costs and burdens on the Internet providers whose domain names they use. First, misaddressed emails, which ordinarily are automatically returned to sender, are routed to the false return address used by the spammer. Since the user id typically does not exist, rather than being returned to a specific email box, the misaddressed email is routed to the postmaster or network supervisor of the server attached to the false return address, who may open the message to try to determine where to reroute it. Second, recipients of junk email often respond by flaming – or sending angry return email messages to – authors of junk email messages; when a false return address is used, these messages, as well, are routed to the network supervisor of the domain name used by the spammer as its false return address.

B. CAN SPAM Act

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) preempts state laws (other than those dealing with fraud and deception) and regulates senders and advertisers with respect to *commercial* email messages, which is defined as those messages that have a *primary purpose* of advertising or promoting a product or service (including online content). The statute excludes *transactional or relationship messages*, which are those that have a *primary purpose* of (1) facilitating a commercial transaction already agreed to by the recipient; (2) providing warranty, product recall, safety or security information; (3) communicating information relating to an employment relationship; (4) delivering goods or services which the recipient is entitled to receive under the terms of a transaction; or (5) notifying the recipient of a change in the terms or features of, or of recipient's standing with respect to, or at regular

intervals account balance information or other types of account statements with respect to, a subscription, membership, account, loan, or comparable ongoing relationship. Transactional or relationship messages are not subject to the CAN-SPAM Act except to the extent they may contain false or misleading header information.

The Act requires that commercial email messages *clearly and conspicuously* include information such as a functional return email address or other mechanism to allow recipients to opt-out, a valid physical world address, a notice that the message constitutes an advertisement or solicitation and (in the case of sexually oriented communications) certain additional disclosures.

The Act prohibits false and misleading header information, misleading RE line descriptions, harvesting email addresses and various techniques used by spammers to mask their true identity.

The CAN-SPAM Act may be enforced by federal government agencies, State Attorneys General and ISPs. Except for ISPs, there is no private cause of action authorized by the statute.

Penalties under the Act include fines of up to $2 million (which potentially may be tripled for willful, knowing, or aggravated offenses) and up to five years in prison.

Some of the specific terms of the statute (such as *primary purpose*) have yet to be specifically defined by the FTC. See Ian C. Ballon, *E-Commerce and Internet Law*, Chapter 34 (Glasser LegalWorks 2001 & 2004 Cum. Supp.).

C. Case Law

1. America Online, Inc. v. Cyber Promotions, Inc. Cyber Promotions, a company that distributes mass emailings on behalf of its commercial customers, filed suit against America Online, alleging that AOL had tried to put it out of business by sending it "email bombs." America Online responded that it was a violation of AOL's terms and conditions to distribute mass emailings from an AOL account. America Online subsequently filed its own suit against Cyber Promotions, Inc., alleging that Cyber Promotions, Inc. used forged return addresses in its mailings, including *aol.com*, to avoid detection, and that AOL's postmaster workstation was overwhelmed with returned email messages bearing the forged addresses. On April 11, 1996, the parties stipulated to a preliminary injunction barring Cyber Promotions, Inc. from using any of America Online's trademarks, including its *aol.com* domain name, in junk email communications. America Online, Inc. v. Cyber Promotions, Inc., Civil Action No. C-96-4621 (E.D. Va. 1996).

In a later ruling, granting in part AOL's motion for summary judgment, the court held that Cyber Promotions did not have a First Amendment right to send unsolicited email over the Internet to subscribers of a private network because AOL was not equivalent of a state actor. The court also held that AOL could use blocking software to prevent its subscribers from receiving email from Cyber Promotions. Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 436 (E.D. Pa. 1996).

The case settled in February 1997. Cyber Promotions dropped its opposition to AOL's use of PreferredMail, which allows subscribers to decide whether to screen out unsolicited email, and agreed to use only one of five domains to send unsolicited email to AOL's subscribers. In the past, Cyber Promotions had used multiple return email addresses to circumvent PreferredMail. Bob Woods, "America Online & Cyber Promotions Split Court Decision," Newsbytes, Feb. 5, 1997.

2. In CompuServe Inc. v. Cyber Promotions, Inc., Civil Action No. C2-96-1070 (S.D. Ohio T.R.O. entered Oct. 28, 1996), CompuServe brought suit against Cyber Promotions, Inc. and its president for service mark infringement, unfair competition, deceptive trade practices, conversion or trespass to personal property and nuisance, violation of the Computer Fraud and Abuse Act, misappropriation/unjust enrichment, breach of contract and fraud. CompuServe focused in part on Cyber Promotions false use of headers, which are the legends attached to email messages that show the message's point of origin, route traveled and ultimate destination. The Complaint alleged that "[b]ecause electronic mail provides an opportunity to reach a wide audience quickly and at virtually no cost to the sender, some companies have begun using it to distribute advertisements over the Internet, sending the same unsolicited commercial message to hundreds of thousands of Internet users at once." CompuServe analogized the practice to a telemarketer's calls to a cellular telephone user, because CompuServe subscribers are charged for the amount of time they spend online, and subscribers spend wasted time accessing, reading and deleting junk email messages.

On October 28, 1996, Judge Graham issued a temporary restraining order prohibiting the defendants from falsifying the headers on junk email messages to make it appear as though the messages originated from a CompuServe account (which they did not) on the grounds that such falsification causes undeliverable email messages to be returned to the falsified CompuServe account (as well as angry responses from the recipients of such messages). The TRO also prohibits the defendants from falsely configuring their email to make it appear that the messages originate from CompuServe's domain (which, among other things, allows the messages to circumvent blocking filters that some Internet providers and users employ to avoid receiving junk email).

Judge Graham subsequently issued a preliminary injunction on February 3, 1997, prohibiting Cyber Promotions from sending email messages to CompuServe subscribers, on the theory that Cyber Promotions' failure to adhere to CompuServe's request to cease such transmissions constituted common law trespass. CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).

3. In Hotmail Corp. v. Van Money Pie, Inc., 47 U.S.P.Q.2d 1020 (N.D. Cal. 1998), the court held that the plaintiff was likely to prevail on, among other theories, claims based on the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and breach of contract; see also America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998) (granting partial summary judgment against a spammer in part based on the Computer Fraud and Abuse Act).

4. In America Online, Inc. v. Prime Data Systems, Inc., Civil Action No. 97-1652-A, 1998 U.S. Dist. LEXIS 20226 (E.D. Va. Nov. 20, 1998), AOL obtained a default judgment against a group of spammers for violations of the Computer Fraud and Abuse Act, false designation of origin, Virginia common law trespass to chattels, violations of the Virginia Computer Crimes Act and common law conspiracy to commit trespass to chattels and to violate Federal and Virginia statutes. In addition to entering permanent injunctive relief, Magistrate Judge Thomas Rawles Jones, Jr. therefore awarded compensatory damages of $101,400 ($0.00078 x 130,000,000 UBE messages transmitted by defendants and logged by AOL) in addition to awarding attorneys fees under the Lanham Act and punitive damages for trespass to chattels in the amount of $304,200 (treble the amount of compensatory damages). AOL had submitted evidence that it incurred costs of at least $0.00078 per email message sent (exclusive of personnel and other costs tied to the operation of its computers) – or roughly one cent for every 13 messages sent.

5. In Intel Corp. v. Hamidi, 30 Cal. 4th 1342 (2003), the California Supreme Court clarified that to state a claim for electronic trespass in a case involving unauthorized email transmissions directed to a computer network (in this case, Intel's network, which was sent unsolicited communications by a former employee), a plaintiff must show damage to the recipient's computer system or impairment of its functioning.

D. Administrative Regulation

In FTC v. Maher (D. Md. Complaint filed Mar. 4, 1998), the FTC brought suit against a spammer for unfair and deceptive marketing practices to consumers.

As noted above in section B, the FTC has jurisdiction to enforce the provisions of the CAN-SPAM Act.

E. State Regulation

1. State Statutes. Several states have enacted laws regulating the dissemination of unsolicited commercial email. See, e.g., Cal. Bus. & Prof. Code §§ 17511.1, 17538.45; Cal. Penal Code § 502. Some of these statutes have been preempted in whole or part by the CAN-SPAM Act.

2. Litigation. In Engst v. World Touch Networks, No. 98-2-17831-1 (King county, WA Sup. Ct. complaint filed July 17, 1998), a plaintiff brought suit for damages against an alleged spammer under Washington state law.

3. The constitutionality of Washington State's law was upheld in a challenge based on the dormant Commerce Clause. See State v. Heckel, 143 Wash. 2d 824, 24 P.3d 404 (2001), cert. denied, 534 U.S. 997 (2001).

4. California's anti-spamming statute likewise was upheld against Commerce Clause objections. See Ferguson v. Friendfinders, Inc., 94 Cal. App. 4th 1255, 115 Cal. Rptr. 2d 258, review denied, 2002 Cal. LEXIS 2378 (Apr. 10, 2002).

5. State Attorneys General Enforcement Actions. State Attorneys General have authority to initiate enforcement actions under the CAN-SPAM Act.

F. Spoofing. When a phony identity is used by a spammer, satellite litigation may be required to compel disclosure of the true identity of the responsible party. See supra § VIII(G).

X. PRIVACY (AND SECURITY) LAWS AFFECTING THE CONDUCT OF ELECTRONIC COMMERCE

A. Overview

Privacy laws affect the conduct of electronic commerce in at least three important respects. First, the practices of website and database owners with respect to their collection, use and dissemination of personally identifiable information – and the disclosures made about these practices – affect consumer confidence in Internet commerce and are the subject of laws (such as the Online Child Protection Act and EU Privacy Directive) and FTC regulation. Second, laws governing privacy potentially affect employee rights in electronic communications (including email) and an employee's use of the Internet or a company's intranet or extranet. See supra § VIII. Third, publicity rights (which are a form of privacy right) may be important in licensing website content.

U.S. Data privacy law is comprised of a patchwork of constitutional, statutory and common law privacy rights that afford substantial protection in very narrow areas. Privacy rights are recognized under U.S. law in specific circumstances (such as in the context of criminal investigations or in response to intrusive snooping by

strangers), for particular categories of information (such as tax returns, personal financial data or medical records) or for specific classes of people (such as children). By comparison, the protections afforded by U.S. privacy laws are less comprehensive than those mandated by the European Union's Privacy Directive.

Some federal statutes compel particular types of online providers to post specific privacy policies on websites. Such requirements may be imposed in particular on sites that:

- collect information from children (see 15 U.S.C. §§ 6501 to 6506, 16 C.F.R. §§ 312.1 to 312.12)

- constitute "financial institutions" that provide individuals with a financial product or service "primarily for personal, family, or household purposes." (see 15 U.S.C. §§ 6801 *et seq.*; 16 C.F.R. §§ 313.1 to 313.13); or

- "individually identifiable health information" (see 42 U.S.C. § 1320d).

New laws took effect in California in 2004 and 2005, however, that potentially compel all businesses that collect personally identifiable information from California residents to post a privacy policy that complies with California law. See Ian C. Ballon, *E-Commerce and Internet Law*, Chapter 32 (Glasser LegalWorks 2001 & 2004 Cum. Supp.).

If a business posts a privacy policy, its failure to comply with the policy may subject it to FTC enforcement actions.

Increasingly, privacy concerns have been extended to encompass data security. See infra § X(M).

B. The EU Privacy Directive

1. Overview. The EU Privacy Directive compelled EU member states to adopt uniform rules governing data privacy by October 24, 1998. The Directive treats data privacy as a fundamental human right and generally protects personal data collected by governments or for business purposes. Data collected for "purely personal" or "household purposes" is outside the scope of the Directive. See Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive No. 95/46/EC (Oct. 24, 1995). A copy may be obtained at <http://www.open.gov.uk/dpr/insnet2.htm>.

2. Consent or Necessity. Article 7 provides that personal data generally may only be processed where an individual's consent has been obtained or in certain cases of necessity.

a. Consent must be "unambiguously given," specific and informed. A notice buried in website Terms and Conditions will not suffice.

b. Necessity. Personal data alternatively may be processed if one of five conditions are met, such as where processing is necessary for the performance of a contract or to protect the vital interests of the data subject.

c. Free speech. Article 9 also recognizes an exception for the processing of personal data carried out solely for "journalistic purposes or for the purpose of artistic or literary expression . . . ," but only "if they are necessary to reconcile the right to privacy with the rules governing freedom of expression."

d. Special categories. Certain categories of data generally may not be processed absent explicit consent (or may not be processed at all, depending on individual national laws implementing the Directive). These categories of data include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership or disclosing details of a person's health or sex life. See Art. 8.

e. Exemptions. Member states may exempt data processing from the protections of the Directive where necessary to safeguard: national security; defense; public security; the prevention, investigation, detection or prosecution of criminal offenses; important economic or financial interests of the European Union or a member state; certain inspection and regulatory functions; or the protection of the data subject or the rights and freedoms of others. See Art. 13.

3. Data Quality. Article 6 compels member states to assure that personal data is processed fairly and lawfully; collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; accurate, and in certain circumstances kept up to date; and kept in a form which permits identification of individual data subjects only for as long as necessary for the purposes for which the data originally was collected.

4. Mandatory Disclosures. Articles 10 and 11 compel controllers to disclose to data subjects their identities; the purpose for which personal data is being processed; and certain additional information such as whether particular information sought must be provided or is merely optional.

5. The Rights to Access Data and Object to its Processing. Article 12 provides individuals with limited rights to review and correct personal data. Article 14 further provides limited rights to object to the processing

of personal data for direct marketing purposes or on "compelling legitimate grounds."

6. Confidentiality and Security. Data controllers are responsible for ensuring the confidentiality and security of personal data.

7. Transfer of Personal Data to Third Countries. Article 25 restricts the transfer of personal data outside of the EU except where third countries ensure "an adequate level of protection . . ." for personal data, as judged by the standards of the Directive. The United States thus far has been found not to provide an adequate level of protection. This poses potential problems for U.S. businesses – especially those with European operations.

C. The U.S. Response to the EU Privacy Directive

1. Self-regulation. The FTC has encouraged industry self-regulation. The EU has rejected self-regulation as a basis for meeting the requirements of Article 25.

2. Technology. In a June 1998 draft opinion on the Platform for Privacy Preferences (P3P) and Open Profiling Standard (OPS), the Working Party of the Commission concluded that a "technical platform for privacy protection will not in itself be sufficient to protect privacy on the Web. See European Commission Directorate General XV, Working Party on the Protection of Individuals with regard to the processing of Personal Data, Op. 1/98 (June 16, 1998 Draft).

3. U.S. Dept. of Commerce Safe Harbor Principles. In March 2000, the European Union and U.S. Department of Commerce reached agreement on safe harbor principles which, if followed, are intended to allow individual companies a presumption that they provide adequate protections within the meaning of Article 25. See <http://www.ita.doc.gov/td/ecom/menu/html>. Businesses alternatively may enter into the EU Model Contract Clauses or adopt other means of compliance. See Ian C. Ballon, *E-Commerce and Internet Law*, Chapter 32 (Glasser LegalWorks 2001 & 2004 Cum. Supp.).

D. U.S. Constitution

1. Privacy rights under the U.S. Constitution include limited rights that protect individuals from government intrusion. The U.S. Supreme Court has recognized an amorphous, albeit limited, constitutional right to privacy in cases involving personal family matters such as contraception and abortion. See, e.g., Griswold v. Connecticut, 381 U.S. 479 (1965); Roe v. Wade, 410 U.S. 113 (1973).

2. The Fourth Amendment protects individuals' privacy rights against unreasonable searches and seizures and may provide remedies where a person's subjective – yet objectively reasonable – privacy expectations in email have been violated by a government agency acting without a warrant or other permissible grounds for doing so. See, e.g., Minnesota v. Solson, 495 U.S. 91, 95 (1990); United States v. Maxwell, 45 M.J. 406, 417 (Armed Forces Ct. App. 1996).

E. The California Constitutional Right to Privacy

Article I, section 1 of the California Constitution grants California residents an inalienable right to privacy. Unlike the federal Constitutional right to privacy, the state right is express, rather than implied, and was added in 1972 by Proposition 11, a ballot initiative.

1. Personal data. The California right to privacy, which is construed in part based on the arguments advanced in support of the ballot initiative, was directed, among other things, at concerns about entities "gather[ing], keep[ing], and disseminat[ing] sensitive personal information without checking its accuracy or restricting its use to mutually agreed or otherwise legitimate purposes." Hill v. NCAA, 7 Cal. 4th 1, 20, 26 Cal. Rptr. 2d 834 (1994). Initiative proponents also argued that Proposition 11 addressed concerns about "collecting and stockpiling unnecessary information" about individuals, which typically cannot be reviewed and corrected, and "misusing information gathered for one purpose in order to serve other purposes or embarrass" people. Supporters of the initiative specifically cited credit card issuers, insurance companies and employers as entities that collect – and potentially misuse – personal information. Proponents of the initiative also specifically referred to computer-generated data. Hill v. NCAA, 7 Cal. 4th at 21-22, quoting Ballot Pamphlet, Proposed Stats. and Amends. to Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972) 26-27.

2. Not Limited to Government Conduct. Unlike the Fourth Amendment to the federal Constitution, the California right protects California residents in their dealings with both the government and private businesses (including employers).

3. Private Cause of Action. Individuals may bring suit to enforce violations of their rights. In order to state a claim for a violation of California's constitutional right to privacy, a plaintiff must show (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant that constitutes a "serious invasion of privacy." A defendant may avoid liability "by negating any of the three elements . . . or by pleading and proving, as an affirmative defense, that the invasion of privacy is justified because it substantively furthers one or more countervailing interests." A plaintiff, in turn, may

rebut a defendant's assertion of countervailing interests by showing that "there are feasible and effective alternatives to defendant's conduct, which have a lesser impact on privacy interests." Loder v. City of Glendale, 14 Cal. 4th 846, 890-91, 59 Cal. Rptr. 2d 696, cert. denied, 522 U.S. 807 (1997).

F. Common Law

Common law rights of privacy and publicity are based in tort law. Justice Brandeis is generally credited with being the first to articulate a broad theory of a right to privacy in a law review article he authored in 1890. See Warren & Brandeis, "The Right to Privacy," 4 Harv. L. Rev. 193 (1890); Prosser & Keeton, Torts § 117 (5th ed. 1984). The modern law of privacy is traced to William L. Prosser, and an influential law review article he wrote in 1960. Prosser identified four distinct causes of action for invasion of privacy: (1) appropriation of the defendant's name or likeness for commercial benefit; (2) unreasonable intrusion, or intentional interference with a plaintiff's interest in solitude or seclusion (either in his person or in his private affairs); (3) public disclosure of private facts; and (4) publicity which places the plaintiff in a false light. Zacchini v. Scripps-Howard Broadcasting Co., 433 U.S. 562, 571 n.7 (1977), citing William L. Prosser, Privacy, 48 Calif. L. Rev. 383, 389, 403 (1960).

G. Statutes Protecting Privacy Rights

Federal statutes provide privacy rights for specific categories of information such as video rental records (18 U.S.C. § 2710), cable television subscriber information (47 U.S.C. § 551) and a student's educational records (20 U.S.C. § 1232g). Some of the more important statutes relating to electronic commerce are:

1. The Fair Credit Reporting Act. This statute prohibits disclosure of information from a person's credit file (such as credit history or employment data) absent consent. 15 U.S.C. §§ 1681 to 1681u. Non-financial information found in a credit-header (which includes a person's name, aliases, birth date, social security number, current and prior addresses and telephone numbers) is not protected from disclosure by the Act.

2. The Electronic Funds Transfer Act requires that contracts with consumers for electronic funds transfers inform consumers when and how information about them may be disclosed. 15 U.S.C. § 1693.

3. The Child Online Protection Act. The Child Online Protection Act, passed in late 1998, directs the FTC to adopt regulations by November 1999 requiring operators of commercial websites or online services to (1) provide notice on the website of the type of information it collects from children, how it uses such information and what its disclosure

practices are; (2) obtain verifiable parental consent for the collection, use or disclosure of personal information from children; (3) provide certain information to parents, when requested; (4) prohibit conditioning a child's participation in a game or related activity where the child's disclosure of additional personal information "is reasonably necessary to participate in such activity . . . ;" and (5) establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children. The Act will take effect in either April 2000 or April 2001, depending on certain FTC actions taken prior to that time.

4. The Computer Fraud and Abuse Act provides civil and criminal remedies when crackers or others break into a computer network (or exceed authorized access) and obtain financial, medical or other information protected by the Act. See 18 U.S.C. § 1030.

5. The Electronic Communications Privacy Act proscribes the interception of communications while in transit (18 U.S.C. §§ 2510 to 2521) or when stored on a network (18 U.S.C. §§ 2701 to 2711). See supra § VIII(D).

H. FTC Privacy Guidelines for Fair Information Practices in Consumer Transactions

The FTC, in a June 1998 report to Congress, proposed guidelines for fair information practices in consumer transactions. See Privacy Online: A Report to Congress (FTC June 1998). By surveying government studies, both in the United States and other countries, the FTC concluded that it was possible to generalize about core principles of fair information practices. Specifically, the FTC concluded that consumers must be assured:

- *Notice* of an entity's information practices;
- *Choice* with respect to how information collected about them is used and disseminated;
- *Access* to information about them collected and stored by an entity;
- *Security* that a data collector has taken appropriate steps to ensure the security and integrity of any information collected; and
- *Enforcement mechanisms* to ensure compliance with these principles, when adopted in practice codes or guidelines.

I. FTC Enforcement Actions: *In re: GeoCities* and Beyond

The FTC filed a complaint against GeoCities, Inc. alleging that its failure to abide by the terms of its stated privacy policy constituted an unfair or deceptive act or

practice within the meaning of section 5(a) of the Federal Trade Commission Act. In re: GeoCities, File No. 9823015 (F.T.C. 1998).

GeoCities offers its members free email accounts, free and fee-based personal home pages, contests and children's clubs, among other services. People wishing to obtain free email accounts, personal homepages or other services were required to complete a membership application that included both mandatory and optional information fields. The form also asked applicants to indicate whether they wished to receive "special offers" from advertisers and specific goods or services from individual companies.

1. FTC Allegations. First, the FTC alleged that GeoCities falsely represented that the personal identifying information it collected from membership application forms was used only to provide members the specific advertising offers or goods or services requested. In fact, according to the FTC, GeoCities sold, rented or otherwise disclosed this information to third parties to be used for purposes other than the ones for which permission had been obtained from GeoCities members. Second, the FTC alleged that GeoCities falsely represented that the "optional information" it collected from members was not disclosed to third parties without the member's permission. In fact, the FTC alleged that GeoCities disclosed this information to third parties who used it to conduct targeted advertising to GeoCities members. Third, the FTC alleged that GeoCities falsely represented that it collected and maintained personal identifying information of children who signed up to join the Official GeoCities' GeoKidz Club or to participate in contests. In fact, according to the FTC, such information was collected and maintained by third party "community leaders," who also ran GeoCities' contests.

2. Consent Judgment. A consent judgment entered in August 1998 prohibits GeoCities from making any misrepresentation about its collection or use of personal identifying information from or about consumers, including what information will be disclosed to third parties and how the information will be used. GeoCities agree to provide "clear and prominent notice" to consumers of its data collection practices, including at least the following information:

    - What information is being collected (e.g., "name," "home address," "e-mail address," "age," "interests");
    - Its intended use(s);
    - The third parties to whom it will be disclosed (e.g., "advertisers of consumer products," "mailing list companies," "the general public");

- The consumer's ability to obtain access to or directly access such information and the means by which (s)he may do so;

- The consumer's ability to remove directly or have the information removed from respondent's databases and the means by which (s)he may do so; and

- The procedures for having personal identifying information deleted from GeoCities' databases and any limitations imposed on such deletion.

The Consent Judgment also contained specific requirements on how GeoCities' new privacy policy would be posted on its website. GeoCities further agreed that it would not collect personally identifying information from any child age 12 or younger if it has actual knowledge that the child does not have the permission of a parent to provide such information. The Judgment further provides that GeoCities shall not be deemed to have actual information where a child has falsely represented the she is an adult and it has no reason to doubt such information.

3. Checklist for Complying with FTC Guidelines. A checklist for complying with FTC guidelines, drawn from recent enforcement actions, may be found in section 32.12[5][C] of Ian C. Ballon, *E-Commerce and Internet Law* (Glasser LegalWorks 2001 & 2004 Cum. Supp.).

J. Collection of Information from California Residents

California has enacted three laws governing the collection of information from California residents that businesses that operate on a nation-wide basis must comply with. Additional information on California laws may be found in section 32.13[6] of Ian C. Ballon, *E-Commerce and Internet Law* (Glasser LegalWorks 2001 & 2004 Cum. Supp.).

1. California's Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575 *et seq.,* which took effect on July 1, 2004, requires operators of commercial Web sites and online services that collect personally identifiable information about California residents over the Internet or online to conspicuously post a privacy policy that includes specific information mandated by the statute.

2. California Civil Code section 1798.81.5, which took effect on January 1, 2005, requires most businesses that own or license personal information about California residents to implement and maintain reasonable security procedures to protect personal information from unauthorized access, destruction, use, modification or disclosure, and to contractually bind third parties who obtain this information to maintain reasonable security

procedures. California previously had adopted a security notification statute. See infra § X(M).

3. California Civil Code sections 1798.83 and 1798.84, which took effect on January 1, 2005, require businesses that disclose personal information to third parties for direct marketing purposes to make certain disclosures to consumers and, upon request, provide them with details about the specific information disclosed about them.

K. Federal Regulatory Jurisdiction

1. Opt-in vs. opt-out procedures. Internet marketers prefer procedures that compel users to affirmatively opt-out of marketing programs. The EU, by contrast, generally requires that consumers be given the choice to opt-in before their data can be used. In different statutes, Congress has adopted both opt-in (in the case of the Driver's Privacy Protection Act) and opt-out provisions (under the Gramm-Leach-Bliley Act).

2. The Commerce Clause. In Reno v. Condon, 528 U.S. 141 (2000), the U.S. Supreme Court gave broad approval to the power of Congress to regulate privacy issues pursuant to its authority over interstate commerce. The case concerned the Driver's Privacy Protection Act of 1994 (codified at 18 U.S.C. §§ 2721 to 2725), which prohibits state departments of motor vehicles (DMVs) or their employees or contractors (subject to specific exceptions) from knowingly disclosing or otherwise making available to any person or entity personal information about any individual obtained in connection with a motor vehicle record. The Court upheld the constitutionality of the Act even though it conflicted with a South Carolina statute that allowed DMV data to be freely marketed to third parties, because the Court concluded that "[t]he motor vehicle information which the States have historically sold is used by insurers, manufacturers, direct marketers, and others engaged in interstate commerce to contact drivers with customized solicitations" and therefore constituted "an article of commerce," the "sale or release into the interstate stream of business is sufficient to support congressional regulation." In so ruling, Chief Justice Rehnquist, writing for a unanimous Court, rejected South Carolina's Tenth Amendment arguments, because "the DPPA does not require the States in their sovereign capacity to regulate their own citizens. The DPPA regulates the States as owners of databases." Id. at 671, 672.

3. First Amendment Limitations. While Congress undoubtedly could compel use of opt-in procedures pursuant to its power to regulate data in interstate commerce, there is at least some question about whether the FTC could do so in implementing more general federal privacy guidelines. See U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999) (invalidating under the First Amendment an opt-in procedure adopted by the FCC to protect unspecified privacy interests), cert. denied, 530 U.S. 1213 (2000).

L. Website, E-Commerce and Class Action Litigation

1. In re Pharmatrak Privacy Litig., 329 F.3d 9 (1st Cir. 2003). The court reversed (and remanded for further consideration) the entry of summary judgment on plaintiffs' claim under the Electronic Communications Privacy Act (ECPA) that their privacy rights had been violated when the defendants' practice of collecting personal information on websites was not disclosed to users.

2. In In re Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001), the court granted defendant's motion to dismiss plaintiffs' federal claims, declined to exercise supplemental jurisdiction over plaintiffs' state law claims, and dismissed with prejudice plaintiffs' amended complaint based on various claims arising out of Doubleclick's proposed plan to allow participating websites to exchange cookie files obtained by users to better target banner advertisements. Plaintiffs, web users, had alleged that defendant's cookies collected information about them, such as names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the internet, and web pages or sites, which plaintiffs considered personal in nature and that users would not ordinarily expect advertisers to be able to collect. Among other things, the court ruled that because defendant's affiliated web sites were the relevant "users" of internet access under the Electronic Communications Privacy Act (ECPA), and submissions containing personal data made by users to defendant's affiliated web sites were intended for those websites, the sites' authorization was sufficient to grant defendant's access under 18 U.S.C. § 2701(c)(2).

3. In In re Toys R Us, Inc. Privacy Litig., MDL No. M-00-1381, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. Oct. 9, 2001), the court found that plaintiffs had stated a claim under the Computer Fraud and Abuse Act and granted leave to amend to assert a Wiretap Act claim in a case based on the defendant's alleged use of cookies to collect user data.

4. The court in In re Intuit Privacy Litig., 138 F. Supp. 2d 1272 (C.D. Cal. 2001) dismissed cookie-related privacy claims brought under 18 U.S.C. § 2520 and 18 U.S.C. § 1030, but denied defendant's motion with respect to plaintiffs' section 2701 claims related to stored data.

5. Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001). The court granted summary judgment for the defendants and denied plaintiffs' motion for class certification as moot in a case arising out of defendants' alleged placement of cookies on user computers, permitting user communications to be monitored allegedly without their knowledge. The court granted summary judgment on plaintiffs' Computer Fraud and Abuse Act claim because the minimum $ 5,000 damage requirement had not been met. The court further granted summary judgment on plaintiffs'

claim under the Stored Communications Act, 18 U.S.C. § 2701 *et seq*. because, given the technological and commercial relationship between users and the defendant's website, it was implausible to suggest that "access" was not intended or authorized. Summary judgment likewise was granted on plaintiffs' claim under the Wiretap Act, 18 U.S.C.S. § 2510 *et seq*. based on the finding that it was implicit in the code instructing users' computers to contact the web site that consent had been obtained to the interception of communication between users and defendants.

6. Supnick v. Amazon.com, Inc., 2000 U.S. Dist. LEXIS 7073 (W.D. Wash. 2000). Plaintiffs' motion for class certification was granted in a suit claiming that defendants violated the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq*., and related common law rights, through their collection of personal information on the internet.

7. In re RealNetworks, Inc. Privacy Litig., Civil No. 00 C 1366, 2000 U.S. Dist. LEXIS 6584 (N.D. Ill. May 8, 2000). An intervenor's motion for class certification was denied in one case where the court found that the defendant entered into a contract with putative class members that provided for binding arbitration. But see Specht v. Netscape Communications, Inc., 306 F.3d 17 (2d Cir. 2002) (holding posted terms accessible via a link to not be binding on users because assent was not obtained); Comb v. PayPal, Inc., 218 F. Supp. 2d 1165 (N.D. Cal. 2002) (holding a click-through contract that contained an arbitration provision to be substantively and procedurally unconscionable under California law).

8. Privacy claims against Northwest Airlines were dismissed in Dyer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196 (D.N.D. 2004). In that case, customers of Northwest Airlines alleged that the airline provided NASA with addresses, credit card numbers and travel itineraries without their knowledge and in violation of its privacy policy. The court dismissed the plaintiffs' ECPA claim because the sale of services over the Internet was not within the scope of the Act. The court similarly dismissed plaintiffs' breach of contract claim because the privacy policy did not give rise to a contract claim and the plaintiffs did not allege that they in fact had accessed, read, or relied upon the privacy policy, and did not allege any contractual damages arising from the alleged breach.

9. For a discussion of privacy rights in pseudonymous communications, see supra § VIII(G).

M. Internet Security

1. Overview of security law. As noted earlier in this outline, "Internet security" usually refers to three separate issues from a legal perspective: (1) gateway security (or the security at the point where a company's computers are potentially accessible to third parties); (2) Internet security

(where federal law generally prohibits the unauthorized interception of communications); and (3) internal security. *See* Ian C. Ballon, *E-Commerce and Internet Law*, Chapter 4 (Glasser LegalWorks 2001 & 2004 Cum. Supp.).

Security today is a field that resembles privacy law in 1995, when there was a patchwork of remedies available under state law or specific federal statutes and the FTC had just begun to study online privacy issues pursuant to its broad jurisdiction over unfair or deceptive consumer practices. As with privacy in 1995, security today is an area where engineers and technological solutions, more than legal standards, define the practices of most businesses. Federal law imposes security obligations on businesses in a limited number of specific fields (such as financial services and health care), state legislators are beginning to consider online security as an important issue (following California's adoption of a security reporting statute, which took effect in 2003) and the FTC is focusing increasing attention on security as an important aspect of privacy protection.

Although various proposals have been advanced, there is no single U.S. or international standard that, if complied with, could insulate a company from state, federal or regulatory liability. In addition, as with privacy law, technological innovations will continue to change the definition of "reasonable conduct" and effectively will impose new obligations on companies to protect the security of digital information.

Just as privacy law has developed over time, the coming years will see an increase in security-related legislation and litigation, including class action litigation. Businesses should anticipate these trends and adjust their internal practices accordingly.

2. Federal statutes. As with privacy law, federal law imposes only limited security obligations on businesses.

   a. Gramm-Leach-Bliley Act of 1999 (15 U.S.C. §§ 6801-6809, 6821-6827 (2004)). Each financial institution has an affirmative, continuing obligation to protect the confidentiality of customer nonpublic personal information. The statute conditions financial institution disclosure of customer nonpublic personal information to a nonaffiliated third party upon compliance with consumer notification requirements that include: (1) clear, conspicuous disclosures that such information may be disseminated to third parties; and (2) consumer opportunity to prevent such dissemination. In addition, the statute prohibits a financial institution from disclosing a consumer's access number or code to a nonaffiliated third party for use in telemarketing, direct mail

marketing, or other marketing through electronic mail to the consumer.

b. HIPAA Security Rule (45 C.F.R. § 164.312 (2004)). The Security Rule, issued by HHS in 2003 pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), obligates health plans, healthcare clearinghouses and most health care providers (referred to as "covered entities") to employ certain administrative, physical and technical safeguards to ensure the confidentiality and integrity of electronic protected health information. In addition, the Security Rule requires covered entities to appoint a single security official to oversee compliance.

Covered entities must comply with the Security Rule by April 21, 2005. However, the Privacy Rule, which took effect on April 14, 2003, imposes some overlapping obligations, including a general requirement that covered entities adopt "administrative, physical and technical safeguards" to maintain the privacy of protected health information. The Security Rule is organized around general "standards," many of which are divided into more detailed "implementation specifications." While covered entities must comply with all required specifications, with respect to addressable specifications, covered entities may:

(i) Assess whether the specification is reasonable and appropriate given the environment in which the entity is operating;

(ii) If deemed to be reasonable and appropriate, implement the specification;

(iii) If deemed not to be reasonable and appropriate, document the reasons for this determination and implement an equivalent, alternative security measure that is reasonable and appropriate.

Addressable specifications include, among others, encryption, employee access authorization procedures, security reminders, virus protection, log-in monitoring, password management policies and testing/revision of contingency plans. The Security Rule is intended to be "scalable" (i.e., covered entities may develop reasonable, individually tailored approaches to security).

The reasonableness of a particular security measure will be judged by:

(i). The size, complexity and capabilities of the covered entity;

(ii). The covered entity's technical infrastructure, hardware and software capabilities;

(iii). The cost of alternative security measures; and

(iv). The probability and severity of potential risks.

The preamble to the Security Rule emphasizes that risk analysis and risk management form "the foundation on which all of the other standards depend."

3. State laws. There is only limited state regulation of security issues. The most significant state statute is CAL. CIV. CODE §§ 1798.29, 1798.82, which requires a state agency or a person or business that conducts business in California and owns or licenses computerized data that includes personal information, to disclose in specified ways, any security breach to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notifications may be delayed if a law enforcement agency determines that it would impede a criminal investigation. The statute also requires an agency, person, or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any security breach. The bill preempts local regulations, if any. *Notice* may be provided by one of the following methods: (1) Written notice; (2) Electronic notice, if consistent with the provisions regarding electronic records and signatures set forth in the federal eSIGN law (15 U.S.C. § 7001); or (3) Substitute notice, if the person, business, or agency demonstrates that the cost of providing actual notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or that the person, business, or agency does not have sufficient contact information. Substitute notice must include: (A) email notice when the person, business, or agency has an e-mail address for a person; (B) conspicuous posting of the notice on the person, business, or agency's website; or (C) notification to major statewide media.

California Civil Code section 1798.81.5, which took effect on January 1, 2005, further requires most businesses that own or license personal information about California residents to implement and maintain reasonable security procedures to protect personal information from unauthorized access, destruction, use, modification or disclosure, and to contractually bind third parties who obtain this information to maintain reasonable security procedures.

4. FTC Enforcement Actions. The FTC increasingly is considering security in connection with its jurisdiction over unfair or deceptive consumer practices and privacy. The FTC's position on information security, as

articulated in November 2003, is set forth at http://www.ftc.gov/opa/2003/11/cybersecurity.htm. Significant enforcement actions include:

a. Guess, Inc., 2003 F.T.C. LEXIS 85 (2003). In June 2003, Guess settled charges that security flaws had exposed consumers' credit card information to hackers. The FTC alleged that Guess did not use reasonable and appropriate security measures to protect the confidentiality of the collected information. As part of the settlement, Guess agreed to implement a comprehensive information security program. *See* http://www.ftc.gov/opa/2003/06/guess.htm

b. Microsoft, Inc,. 2002 F.T.C. LEXIS 43 (2002). In August 2002, Microsoft settled with the FTC in response to an allegation that Microsoft made false security and privacy promises regarding its "Passport" web services. Microsoft's Passport stores and collects personal and financial information, allowing users to conduct online transactions without separating inputting this data on each website. Among other charges, the FTC alleged that Microsoft's privacy policy falsely represented that Microsoft employed reasonable and appropriate security measures to protect the confidentiality of collected information. As part of the settlement, Microsoft agreed to implement a comprehensive information security program, certified by an independent third party, which would meet or exceed the security standards set forth in the consent order. *See* http://www.ftc.gov/opa/2002/08/microsoft.htm

c. Eli Lilly and Company, 2002 F.T.C. LEXIS 22 (2002). In January 2002, Eli Lilly settled charges with the FTC after it sent an email to Prozac users (reminding them to refill their prescriptions) where recipients were identified in the "TO" line, rather than the "BCC" line. Although the disclosure was unintentional, Eli Lilly agreed to take appropriate steps to ensure the security of the identity of recipients in the future. *See* http://www.ftc.gov/opa/2002/01/elililly.htm.

d. In the Matter of MTS, Inc., File No. 032 3209 (consent order entered June 2, 2004). The FTC alleged that a security flaw in the Tower Records Web site exposed customers' personal information to other Internet users. Tower's privacy policy made claims such as "We use state-of-the-art technology to safeguard your personal information," and "Your TowerRecords.com Account information is password-protected. You and only you have access to this information." When Tower redesigned its site, however, it introduced a security vulnerability that allowed Web users to access Tower's order history records and view certain personal

information about other Tower customers, such as their names, billing and shipping address, email addresses, phone numbers, and their past Tower purchases. The FTC complaint charged that the security flaw was easy to prevent and fix, but that Tower failed to implement appropriate checks and controls in the process of writing and revising its Web applications; adopt and implement policies and procedures to test the security of its Web site; and provide appropriate training and oversight for its employees. It charged that Tower's privacy policy assurances were therefore false and violated the FTC Act. The settlement barred future misrepresentations, required Tower to implement an appropriate security program, and required audits of its Web site security every two years by a qualified third-party security professional for ten years.

e. In the Matter of Petco Animal Supplies, Inc., File No. 032 3221 (consent order entered Nov. 8, 2004). The FTC alleged that Petco failed to implement reasonable and appropriate security measures to protect sensitive consumer information on its Web site, including simple, readily available defenses that would have blocked Structured Query Language (SQL) injection attacks. The FTC alleged that this constituted a deceptive practice in view of security claims Petco made on its Web site, including that "[a]t Petco.com, protecting your information is our number one priority, and your personal information is strictly shielded from unauthorized access" and "[e]ntering your credit card number via our secure server is completely safe. The server encrypts all of your information; no one except you can access it." Petco's settlement with the FTC prohibited Petco from misrepresenting the extent to which it maintains and protects sensitive consumer information. It also required Petco to establish and maintain a comprehensive information security program designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Petco agreed to arrange biennial audits of its security program by an independent third party certifying that Petco's security program is sufficiently effective to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information has been protected. The settlement also contained record keeping provisions to allow the FTC to monitor compliance.

XI. OBSCENITY AND FREE SPEECH

A. Child Pornography

1. Distribution and possession illegal. U.S. law prohibits distribution or possession of child pornography. 18 U.S.C. § 2251; Osborne v. Ohio, 495 U.S. 103 (1990). However, this statute was ruled unconstitutional in a case charging purely intra-state conduct. See United States v. Mathews, 300 F. Supp. 2d 1220, 1232 (N.D. Ala. 2004).

2. Reporting Requirement. Pursuant to the Protection of Children from Sexual Predators Act of 1998 and implementing regulations, anyone engaged in providing an *electronic communication service* or a *remote computing service* to the public must report "knowledge of facts or circumstances" from which a violation of child pornography laws is apparent to the National Center for Missing and Exploited Children (NCMEC) and the FBI or U.S. Customs Service. Such a report must be made "as soon as reasonably possible" after obtaining knowledge and should include "whatever information . . . that led it to conclude that a violation of federal child pornography statutes" had occurred. The regulations suggest that a report "could include information concerning: visual depictions of child pornography; the identity of persons or screen names or persons transmitting or receiving child pornography; or requests by persons to receive child pornography." See 42 U.S.C. § 13032(b); 18 U.S.C. § 2702(b)(6); 28 C.F.R. § 81.12. A provider who knowingly and willfully fails to make a required report may be fined up to $100,000 (or $50,000 for an initial violation).

3. Morphing and virtual child pornography.

   a. The Child Pornography Prevention Act of 1996 also made it illegal to receive, reproduce or distribute visual images enhanced to appear as though they depict child pornography (based on Congressional findings that images of young children engaging in sexual acts – whether real or computer-generated – were used by pedophiles to lure children into engaging in these acts). See 18 U.S.C. § 2252A.

   b. Affirmative Defense. The Act created an affirmative defense where the alleged child pornography was created using actual people who were adults at the time the material was produced and "the defendant did not advertise, promote, present, describe, or distribute the material in such a manner as to convey the impression that it is or contains a visual depiction of a minor engaging in sexually explicit conduct." Id. § 2252A(c).

c. Supreme Court Ruling. The U.S. Supreme Court ruled that the Act's ban on sexually explicit images that appeared to depict minors, but which were not produced using minors, was unconstitutionally overbroad. See Ashcroft v. The Free Speech Coalition, 535 U.S. 234 (2002).

B. Interstate Transportation of Obscene Material

1. Transportation and distribution prohibited. U.S. law prohibits the transportation, distribution or importation of obscene material, which is not protected by the constitutional guarantees of freedom of speech or freedom of press. 18 U.S.C. §§ 1462, 1465; Roth v. United States, 354 U.S. 476 (1957). In Stanley v. Georgia, 394 U.S. 557 (1969), the U.S. Supreme Court held that individuals have a privacy right to possess obscene materials in their homes. In subsequent decisions, however, the Court has clarified that this right does not create a correlative right to receive, transport or distribute obscene material in interstate commerce.

2. In United States v. Maxwell, 45 M.J. 406 (U.S. Armed Forces Ct. App. 1996) the court upheld the court martial conviction of Col. Maxwell for violating federal law by using his personal computer (a) to receive or transport visual depictions of minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252 and (b) to transport in interstate commerce, for the purpose of distribution, visual depictions of an obscene, lewd, lascivious or filthy nature in violation of 18 U.S.C. § 1465. The court reversed the defendant's earlier conviction for using his personal computer to communicate indecent language to another service member via email on his America Online account. The offending conduct occurred on the defendant's home computer during off-duty hours.

3. United States v. Chapman, 60 F.3d 894 (1st Cir. 1995). The defendant pled guilty to transporting child pornography in interstate commerce in violation of 18 U.S.C. § 2252(a)(1) for transmitting over America Online to an AOL subscriber in another state three photographs depicting children engaged in sexual acts. In an appeal of his sentence, the First Circuit held that the transmission of child pornography by computer is not "sexual abuse or exploitation" within the meaning of the U.S. sentencing guidelines.

4. United States v. Thomas, 74 F.3d 701 (6th Cir. 1996). The defendants were convicted for violating the federal obscenity laws in connection with their operation of a BBS that allowed subscribers to download images and order videotapes by mail of material found to be obscene.

C. The Communications Decency Act: *Indecent* and *Patently Offensive* Communications Directed at Minors

In Reno v. ACLU, 521 U.S. 844 (1997), the U.S. Supreme Court struck down those provisions of the Communications Decency Act ("CDA") which restricted access by interactive computer service to *indecent* and *patently offensive* communications as an unconstitutional abridgement of free speech. The Court left intact section 223(a) to the extent it applies to "any comment, request, suggestion, proposal, image or other communication which is obscene . . . as opposed to merely indecent."

1. Vagueness. The Court found the CDA impermissibly vague, in part because different terminology was used in two parallel sections of the CDA (*indecent* in 47 U.S.C. § 223(a) and material that "in context, depicts or describes, in terms *patently offensive* as measured by contemporary community standards, sexual or excretory activities or organs" in subsection (d)). The Court wrote that it was unclear how these two standards (which were taken from elements of previous Supreme Court tests) related to one-another or just what they meant. For example, although the *patently offensive* language used in the statute was taken from one of the three prongs of the definition for obscene material adopted by the Court in Miller v. California, 413 U.S. 15 (1973), the Court wrote that "[j]ust because a definition including three limitations is not vague, it does not follow that one of those limitations, standing by itself, is not vague."

2. Breadth. In ruling that the CDA failed to pass strict scrutiny, the Court emphasized that "[t]he breadth of the CDA's coverage is wholly unprecedented" and therefore "impose[d] an especially heavy burden on the Government to explain why a less restrictive provision would not [have] be[en] as effective as the CDA." The Court noted that the CDA was not limited to commercial speech (and therefore burdened nonprofit organizations and individuals, as well as businesses) and – by virtue of the definitions of *indecent* and *patently offensive* – "cover[ed] large amounts of nonpornographic material with serious educational or other value." The Court further noted that the "community standards" criterion "as applied to the Internet means that any communication available to a nation-wide audience will be judged by the standards of the community most likely to be offended by the message." In addition, the Court also pointed out the absence of congressional findings made it more difficult to conclude that Congress had carefully considered whether less restrictive measures were available.

3. Justice O'Connor's Zoning Analysis. Justice O'Connor, joined by Chief Justice Rehnquist, concurred in part and dissented in part, analyzing the CDA as a legitimate attempt "to create 'adult zones' on the Internet." Justice O'Connor found the CDA lacking, however, to the extent that it substantially interfered with the First Amendment rights of adults. She

would have invalidated the "display" and "indecency transmission" and "specific person" provisions of the "patently offensive" prong as applied to communications involving more than one adult, but would have upheld the "indecency transmission" and "specific person" provisions insofar as they applied to communications between a single adult and one or more minors.

Justice O'Connor wrote that adult zoning laws have been sustained under the First Amendment if: (1) they do not unduly restrict adult access to the material; and (2) minors have no First Amendment right to read the material.

D. The Child Online Protection Act: Commercial Speech Deemed *Harmful to Minors*

In October 1998, Congress enacted the Child Online Protection Act, 47 U.S.C. § 231 (colloquially referred to as "CDA II" since it reflects an attempt to meet some of the objectives of the Communications Decency Act held unconstitutional in Reno v. ACLU, 521 U.S. 844 (1997), while also responding to the specific defects noted by the Supreme Court in that case).

1. Harmful to minors. The Act is more narrowly tailored than the CDA and merely regulates the knowing commercial dissemination of content "harmful to minors," when made freely available over the Internet by commercial vendors of adult content. The statute only applies to commercial speech, which is entitled to a lower level of First Amendment protection than other forms of speech, and incorporates the "harmful to minors" or "obscene as to children" standard upheld in the context of magazine vendors in Ginsberg v. New York, 390 U.S. 629 (1968).

2. ISP Exemption. Among other things, the statute exempts "a person engaged in the business of providing an Internet access service . . . ." 47 U.S.C. § 231(b)(2).

3. Enforcement enjoined. The U.S. Supreme Court rejected the ACLU's challenge that the statute's reliance on community standards to identify material harmful to minors violated the First Amendment, but expressed no view with respect to other potential challenges to the statute. See Ashcroft v. ACLU, 535 U.S. 564 (2002). However, in Ashcroft v. ACLU, 124 S. Ct. 2783 (2004), the U.S. Supreme Court upheld a preliminary injunction against enforcement of the statute on the grounds that less restrictive alternatives exist.

E. Screening Software

1. In United States v. American Library Association, 539 U.S. 194 (2003), the U.S. Supreme Court upheld the Constitutionality of the Children's

Internet Protection Act, which requires public libraries to use filtering software to prevent access to materials harmful to minors as a condition of obtaining federal funding.

2. In Mainstream Loudoun v. Loudoun County Library, 24 F. Supp. 2d 552 (E.D. Va. 1998), Judge Leonie Brinkema granted summary judgment in favor of the plaintiffs, finding that a public library's use of screening software violated the First Amendment. She wrote that while the library was "under no obligation to provide Internet access to its patrons," once it decided to do so the First Amendment restricted its ability to limit patrons' access.

F. State Regulation of the Internet

1. American Library Association v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997). In a ruling issued just days before the U.S. Supreme Court struck down most of the CDA in Reno v. ACLU, a lower court in New York entered a preliminary injunction barring enforcement of N.Y. Penal Law § 235.21(3) which, like the CDA, prohibited certain forms of inappropriate communications directed at minors. The court's decision, however, turned on the dormant Commerce Clause, rather than the First Amendment. The court found that, because geographic boundaries do not exist in cyberspace, the statute represented an unconstitutional projection of New York law into conduct that occurs wholly outside of the state. In addition, the court concluded that the burdens imposed by the law on interstate commerce outweighed any local benefit derived from it. Finally, and perhaps most dramatically, the court concluded that the Internet "requires a cohesive national scheme of regulation . . . " and that "[t]he need for uniformity in this unique sphere of commerce requires that New York's law be stricken as a violation of the Commerce Clause." The dormant Commerce Clause has also served as the basis for striking down other state laws regulating the Internet. See, e.g., PSINet, Inc. v. Chapman, 167 F. Supp. 2d 878 (W.D. Va. 2001) (criminal statute prohibiting dissemination of material harmful to minors), aff'd, 362 F.3d 227 (2004); Cyberspace Communications, Inc. v. Engler, 142 F. Supp. 2d 827 (E.D. Mich. 2001) (similar). But see State v. Heckel, 143 Wash. 2d 824, 24 P.3d 404 (2001) (upholding Washington's anti-spamming statute against a challenge that it violated the dormant Commerce Clause), cert. denied, 534 U.S. 997 (2001); Ferguson v. Friendfinders, Inc., 94 Cal. App. 4th 1255, 115 Cal. Rptr. 2d 258 (upholding the constitutionality of California's anti-spamming statute), review denied, 2002 Cal. LEXIS 2378 (Apr. 10, 2002).

2. ACLU v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997). A federal court in Atlanta entered a preliminary injunction barring enforcement of a Georgia statute which made it a crime for any person to knowingly transmit data over a computer network using a false identification or knowingly using a

third party's trade name, registered trademark, logo, legal or official seal, or copyrighted symbol to falsely state or imply that such person had permission or was legally authorized to do so. In a decision rendered just days before the U.S. Supreme Court issued its opinion in Reno v. ACLU, the court found the law to be an impermissible content-based restriction on speech, overly broad and unconstitutionally vague.

3. In Urofsky v. Gilmore, 167 F.3d 191 (4th Cir. 1999), an appellate panel reversed a ruling by District Court Judge Leonie Brinkema that had struck down a Virginia statute that restricted the ability of state employees to access sexually explicit material on state owned or leased computers. A petition for certiorari (following affirmance by *en banc* review) was denied.

4. In ACLU v. Johnson, 194 F.3d 1149 (10th Cir. 1999), the court enjoined enforcement of a New Mexico statute intended to protect children from sexually explicit Internet content, finding the law unconstitutional under the First, Fifth and Fourteenth Amendments and the Commerce Clause of the U.S. Constitution.

G. International Regulation

A number of countries regulate material more strictly than the United States. Certain countries, however, act as data havens, where even child pornography is not prosecuted.

XII. INTERNET CRIMES

A. Criminal Copyright Infringement. See supra § I(I).

B. Computer Fraud and Abuse Act of 1986

1. 18 U.S.C. § 1030(a)(5)(A) penalizes "anyone who intentionally accesses a Federal interest computer without authorization, and by means of one of more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information . . ." and thereby causes loss of $1,000 or more.

2. In United States v. Morris, 928 F.2d 504 (2d Cir.), cert. denied, 502 U.S. 817 (1991), the Second Circuit upheld the conviction under this act of Robert Morris, a Cornell graduate student who released the Internet "worm," which was a virus that replicated itself multiple times over the Internet causing computers around the country to crash, including government computers.

C. Threats Transmitted Via Email

1. United States v. Baker, 890 F. Supp. 1375 (E.D. Mich. 1995), aff'd sub nom. United States v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997).

   a. Indictment quashed. The court granted the defendant's motion to quash his indictment under 18 U.S.C. § 875(c) for five counts of transmitting threats to injure or kidnap another in email messages transmitted over the Internet to "Gonda," an anonymous cyberfriend in Canada. Baker had posted a "rape fantasy" story to an Internet newsgroup, which graphically described the torture, rape and murder of a woman who was given the name of a classmate of Baker's at the University of Michigan. During the course of the investigation into this incident, Baker consented to a search of email messages stored on the hard drive of his dormitory room computer.

   b. Threats too remote. The court determined that the messages sent by private email did not amount to threats when evaluated in light of their foreseeable recipient (an anonymous email correspondent). As an illustration of the potential difficulties associated with applying existing laws to cyberspace, the court wrote that "'he' could be a ten year old girl, an eighty year old man, or a committee in a retirement community playing the role of Gonda gathered around a computer."

2. Stalking laws. Sending harassing email messages could violate California's stalking law or analogous statutes enacted in other states. See Cal. Penal Code § 646.9 (declaring it illegal to willfully, maliciously and repeatedly follow or harass another person and make a credible threat with intent to place that person in reasonable fear of death or bodily injury); McGraw, "Sexual Harassment in Cyberspace: The Problem of Unwelcome E-mail," 20 Rutgers Computer & Tech. L.J. 491 (1995).

D. Trade Secrets

The Economic Espionage Act of 1996 criminalized wrongful copying or control of trade secrets. 18 U.S.C. § 670.

1. A trade secret is defined under the Act to mean all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public . . .

2. The statute criminalizes two types of misappropriations where the defendant has "wrongfully copie[d] or otherwise control[led] a trade secret, or attempt[ed] or conspire[d] to do so . . ." First, the law proscribes wrongful copying or control where the defendant has reason to believe that the offense will, or where the defendant actually intends to, "benefit any foreign government, foreign instrumentality, or foreign agent . . . " Second, the statute prohibits wrongful copying or control "with the intent to divert a trade secret, that is related to or is included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and with the intent to, or reason to believe that the offense will, disadvantage any owner of the trade secret . . . ." 18 U.S.C. § 670(a).

E. The National Stolen Property Act

1. Electronic theft covered by the act: United States v. Riggs, 739 F. Supp. 414 (N.D. Ill. 1990).

a. Facts: Neidorf and Riggs accessed Bell South's computer and transferred certain files via modem to Neidorf's computer. Defendants were convicted under 18 U.S.C. § 2314 for theft of electronic text files.

b. Conviction. The court reasoned that because "[i]t is well-settled that when proprietary business information is affixed to some tangible medium, such as a piece of paper, it constitutes 'goods, wares or merchandise' within the meaning of Section 2314, and because Riggs' conduct clearly would have come within the statute if the files he had stolen had been affixed to a floppy disk or printed in hard copy, "[t]his court sees no reason to hold differently simply because Neidorf stored the information inside the computer instead of printing it out on paper. In either case, the information is in a transferable, accessible, even salable form." Id. at 420-21. In the alternative, the court ruled that the information was tangible property:

> Although not printed out on paper, a more conventional form of tangibility, the information in Bell South's E911 text file was allegedly stored on a computer. Thus, by simply pressing a few buttons, Neidorf could recall that

information from computer storage and view it on his computer terminal.

c. First Amendment defense rejected. Riggs' First Amendment defense subsequently was rejected in Riggs v. United States, 743 F. Supp. 556 (N.D. Ill. 1990).

2. Electronic theft not covered by the Act: United States v. Brown, 925 F.2d 1301 (10th Cir. 1991).

a. Holding: The Tenth Circuit held that a computer program (including source code and documentation) were intangible property and, as such, did not constitute "goods, wares, merchandise, securities or monies" which had been stolen within the meaning of the National Stolen Property Act, 18 U.S.C. §§ 2311 et seq. 925 F.2d at 1307-09.

b. *Riggs* analysis rejected. The Tenth Circuit expressly declined to follow United States v. Riggs because it found that the statute covered only *physical*, not intangible "goods, wares [or] merchandise." Id.

F. Wire Fraud

A district court held that a defendant was properly charged under the wire fraud statute for the alleged transmission of computer files containing source code, over the defendant's objection that he should have been charged only with copyright infringement. The court noted that the wire fraud statute, 18 U.S.C. § 1343, contains no requirement that physical goods or money be involved. United States v. Wang, 898 F. Supp. 758 (D. Colo. 1995).

G. Civil Remedies for Unlawful Seizures

Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994).

1. Facts: Steve Jackson Games, Inc. ("SJG") published books, magazines and games and operated a BBS called "Illuminati," which it used to post public information about its business, facilitate testing of games in development and communicate with its customers by email. After obtaining a search warrant based in large part on information about an unrelated BBS, the U.S. Secret Service seized SJG computers, disks and electronic "manuscripts" about to be published and, instead of copying the data and returning it, held onto the material for more than three months. The Secret Service also read and deleted private email messages addressed to BBS subscribers, which had been stored on one of the seized hard disk drives.

2. The Federal Wiretap Act (18 U.S.C. § 2510), as amended by title I of the Electronic Communications Privacy Act of 1986 ("ECPA"), proscribes intentional interceptions of wire, oral or electronic communications. The Fifth Circuit held that the seizure of a computer on which private email has been stored (but not yet retrieved by the intended recipients) does not constitute an unlawful "intercept" under the Federal Wiretap Act.

3. The Privacy Protection Act (42 U.S.C. §§ 2000 et seq.) makes it unlawful for a government employee to seize, in connection with a criminal investigation, any materials "reasonably believed to have a purpose to disseminate to the public a newspaper, broadcast or similar form of public communication . . . ." 42 U.S.C. § 2000aa(a). The trial court previously had found that the Secret Service's failure to promptly make copies of draft magazine articles and a book intended for publication, after being advised that the materials were to be published, constituted a violation of the Act (despite the individual officers' protest that they had no actual knowledge of the Act), justifying an award of $51,040 in damages. 816 F. Supp. 432, 440 (W.D. Tex. 1993), aff'd, 36 F.3d 457 (5th Cir. 1994). The government abandoned its cross-appeal of this issue.

4. Stored Wire and Electronic Communications (18 U.S.C. §§ 2701 et seq.). Title II of the EPCA proscribes unauthorized intentional access to stored electronic communications. The district court previously held that the Secret Service had violated this Act and awarded plaintiffs statutory damages and attorneys' fees. The government abandoned its cross-appeal of this issue.

H. Use of the Internet for Law Enforcement

Just as the Internet may be used to engage in criminal conduct, it may also be used effectively by law enforcement. The first criminal charges brought based on an Internet wire tap were filed in early 1996 by the U.S. attorney in Brooklyn, New York against two Americans and a German national who were charged with illegally making and selling electronic devices and cloning equipment used for cellular telephones. Intellectual Property Lawcast, Jan. 15, 1996. The wiretap was obtained following a complaint by AT&T that cellular telephones programmed with stolen numbers were advertised for sale on a worldwide website. Cyberlex (Jan. 1995), citing The New York Times, Dec. 30, 1995, at A22.

XIII. JURISDICTION

A. Personal Jurisdiction

1. Constitutional Test. A court may exercise "general jurisdiction" over a defendant if the nonresident defendant's activities within the forum are "substantial" or "continuous and systematic." Helicopteros Nacionales de

Colombia, S.A. v. Hall, 466 U.S. 408, 414 n.9 (1984), citing Perkins v. Benguet Consolidated Mining Co., 342 U.S. 437, 445 (1952). Alternatively, a court may obtain "specific jurisdiction" over a nonresident defendant if the defendant has sufficient contacts with the forum state and the cause of action to satisfy the "minimum contacts test" first articulated by the U.S. Supreme Court in International Shoe Co. v. Washington, 326 U.S. 310 (1945). In that case, the Court held that:

> [D]ue process requires only that in order to subject a defendant to a judgment in personam, if he be not present within the territory of the forum, he have certain minimum contacts with it such that the maintenance of the suit does not offend "traditional notions of fair play and substantial justice."

Id. at 316, citing Milliken v. Meyer, 311 U.S. 457, 463 (1940); see also World Wide Volkswagen Corp. v. Woodson, 444 U.S. 286 (1980).

2. Contracts

Jurisdiction often may be found in a dispute between contracting parties brought in the home state of one of the parties to the contract.

a. In CompuServe, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996), the Sixth Circuit held that an Ohio court could assert personal jurisdiction over a Texas resident who had entered into an electronic commercial contract with CompuServe from his home in Texas, to market his shareware software programs.

b. In Hall v. LaRonde, Cal. App. 4th 1342 (1997), a state court in California held that email communications may form the basis for the assertion of jurisdiction.

3. Operation of a website

a. Early decisions held that a defendant's mere operation of a website to promote its business which could be accessed by residents of the forum state, was sufficient to confer specific jurisdiction in a dispute arising out of the domain name used in connection with the site. See, e.g., Inset Systems, Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996); Panavision Int'l, L.P. v. Toeppen, 938 F. Supp. 616 (C.D. Cal. 1996); Maritz, Inc. v. CyberGold, Inc., 947 F. Supp. 1328 (E.D. Mo. 1996).

b. Other courts found jurisdiction proper where a defendant also had more traditional contacts within a jurisdiction. See, e.g., Heroes, Inc. v. Heroes Foundation, 958 F. Supp. 1 (D.D.C. 1996) (newspaper advertisement); Zippo Mfg Co. v. Zippo Dot Com,

Inc., 952 F. Supp. 1119 (W.D. Pa. 1997) (contracts with forum residents and forum subscribers); Digital Equip. Corp. v. AltaVista Technology, Inc., 960 F. Supp. 456 (D. Mass. 1997) (license agreement).

c. *Zippo Dot Com* test. In Cybersell, Inc. v. Cybersell, Inc., 130 F.3d 414 (9th Cir. 1997), the Ninth circuit held that a defendant's mere presence on the World Wide Web was insufficient to confer jurisdiction under the minimum contacts test. Applying the analysis first adopted in Zippo Manufacturing Co. v. Zippo Dot Com., 952 F. Supp. 1119 (W.D. Pa. 1997), the Ninth Circuit distinguished between passive websites, which are merely akin to advertisements, and interactive sites. Under the Zippo Dot Com test, whether jurisdiction may obtain over a defendant based solely on its operation of a website depends on "the level of interactivity and [the] commercial nature of the exchange of information that occurs on the website." 952 F. Supp. at 1124. The Zippo Dot Com test is now applied in some fashion by the Fourth, Fifth, Sixth, Ninth and Tenth Circuits, and multiple district and state courts. See, e.g., ALS Scan, Inc. v. Digital Service Consultants, Inc., 293 F.3d 707, 714-15 (4th Cir. 2002) ("adopting" and modifying the *Zippo Dot Com* formulation in finding that personal jurisdiction could not be asserted over an out-of-state ISP); Mink v. AAAA Development LLC, 190 F.3d 414 (5th Cir. 1999) (finding insufficient interactivity under the *Zippo Dot Com* test for jurisdiction to obtain based on defendant's website); Neogen Corp. v. Neo Gen Screening, Inc., 282 F.3d 883, 890 (6th Cir. 2002) (considering interactivity in connection with purposeful availment); Soma Medical Int'l v. Standard Chartered Bank, 196 F.3d 1292 (10th Cir. 1999) (finding no jurisdiction over a passive website). The District of Columbia Circuit has also applied the test to determine general jurisdiction. See Gorman v. Ameritrade Holding Corp., 293 F.3d 506 (D.C. Cir. 2002).

d. Limitations of the test. Interactivity is merely a proxy for evaluating the nature and quality of the contacts between a defendant, the underlying cause of action and the forum state. The *Zippo Dot Com* test, while widely accepted, does not fully account for all grounds on which jurisdiction may be based. Among other things, the test does not account for physical world contacts and should not be applied to intentional torts or in cases involving transient jurisdiction. See Ian C. Ballon, *E-Commerce and Internet Law - A legal Treatise with Forms,* Chapter 58 (Glasser LegalWorks 2001 & 2003 Supp.).

4. Intentional torts

a. The effects test of Calder v. Jones, 465 U.S. 783 (1984), potentially provides broad grounds for obtaining jurisdiction over out-of-state defendants in cases involving intentional torts such as libel or defamation, cybersquatting cases and other suits involving conduct targeted at the forum state. There is disagreement among circuit courts over the proper scope of the effects test, however, making its applicability to Internet conduct uncertain in some close cases and ultimately dependent in part on where litigation takes place. See Ian C. Ballon, *E-Commerce and Internet Law - A legal Treatise with Forms,* Chapter 58 (Glasser LegalWorks 2001 & 2003 Supp.).

b. In Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316 (9th Cir. 1998), the Ninth Circuit held an out-of-state cybersquatter subject to jurisdiction in California under the effects test of Calder v. Jones.

5. Transient jurisdiction

Regardless of the level of interactivity of a website, personal service on an individual physically present in the jurisdiction, even for a brief period of time, will satisfy due process. See Burnham v. Superior Court, 495 U.S. 604 (1990).

6. *In rem* jurisdiction. Even where personal jurisdiction may be lacking, *in rem* jurisdiction may be asserted over rights to a domain name in a cybersquatting case brought under the Anti-Cybersquatting Consumer Protection Act. See supra § II(C)(3)(c).

7. Recognition of foreign judgments

a. In Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 379 F.3d 1120 (9th Cir. 2004), the court held that there was no personal jurisdiction over a French human rights group that had obtained a judgment against Yahoo! in France relating to Yahoo!'s sale of Nazi memorabilita, thereby vacating the order of District Court Judge Fogel of San Jose that the French court's order (requiring Yahoo! to eliminate Nazi memorabilia from its U.S.-based .com auction site) was unenforceable because it was inconsistent with the First Amendment.

b. Issues involving domestic and international cyberspace jurisdiction are analyzed extensively in chapters 41 and 58 of Ian Ballon, *E-Commerce on Internet Law – A legal treatise with Forms* (Glasser LegalWorks 2001).

B. U.S. Customs Law

Customs exclusion orders barring the importation of products bearing marks identical to registered U.S. trademarks, or protected by U.S. copyrights (15 C.F.R. §§ 133.15 to 133.21 and 133.31 to 133.37) may be rendered meaningless for any goods (such as software) which may be transmitted over the Internet.

C. Criminal Law

In July 1994, Carleen and Robert Thomas, a Milpitas, California couple who operated a BBS that allowed subscribers to download sexually explicit material, were convicted of interstate transportation of obscene material based on their operation of the BBS. The venue for the trial was in the Western District of Tennessee, where a postal inspector initiated a telephone call to the BBS and where community standards were considered to be more likely to favor a conviction. United States v. Thomas, 74 F.3d 701 (6th Cir. 1996).

D. Attorney Advertising

The ethical standards for lawyer advertising are established separately by regulatory authorities in each state. Two states, Texas and Florida, require that home pages be submitted for approval, while other states do not. The jurisdictional reach of these two state requirements beyond attorneys admitted to practice in these jurisdictions may be questionable.

1. Texas. After being chastised in a reported decision for adopting new ethical guidelines that failed to consider advertising over the Internet (Texans Against Censorship, Inc. v. State Bar of Texas, 888 F. Supp. 1328, 1370 (E.D. Tex. 1995), aff'd mem., 100 F.3d 953 (5th Cir. 1996)), the State Bar of Texas adopted a rule requiring Texas lawyers to file a hard copy of their home pages (and printouts showing any subsequent material changes). See State Bar of Texas, Interpretive Comment 17.

2. Florida. Attorneys must submit a hard copy of their homepages, the URL and a check for $100. The Standing Committee on Advertising, "Internet Guideline,"<http://ww3.pwr.com/LEGAL/FLABAR/Regulations/AdReg/adguide.html>.

3. North Carolina. In a proposed ethics opinion, the North Carolina Bar Association concluded that the requirement that attorneys retain records of their advertisements may be satisfied by printing out every single page on a website as launched and all subsequent material changes and retaining the printouts for two years. Proposed RPC 239 (July 25, 1996).

XIV. UPDATE INFORMATION AND NEW CASE LAW

This outline is updated periodically to account for the rapid transformations taking place in the emerging field of Internet law. To request a free update, email your name, address and phone number to iballon@Manatt.com.

IAN C. BALLON is the firm-wide co-chair of the Intellectual Property and Internet Practice Group of Manatt, Phelps & Phillips, LLP, and splits his time between the firm's Los Angeles and Palo Alto offices.

Named one of the top 25 intellectual property lawyers in California in 2003 by *The Daily Journal*, Mr. Ballon concentrates on complex copyright, intellectual property and Internet-related litigation, licensing and strategic counseling for technology, media and entertainment industry clients. Mr. Ballon is the author of the 3-volume legal treatise, *E-Commerce and Internet Law: Treatise with Forms*, published by Glasser LegalWorks (1-800-308-1700 or www.ballononecommerce.com). He is also the Executive Director of Stanford University's Center for E-Commerce and an advisor to the American Law Institute's International Jurisdiction project.

In 1999, Mr. Ballon was named one of the top 20 California lawyers under age 40 by *California Law Business* magazine. In 2001, he was named one of the top new media lawyers in the United States by *CyberEsq.* Magazine and one of the 100 most influential lawyers in California by *California Law Business*. In 2003, he was named by *The Daily Journal* as one of the top 25 copyright, trademark and patent lawyers in California.

Mr. Ballon received an LLM in International and Comparative Law (with an emphasis on international protection of intellectual property) from Georgetown University Law Center and received his JD *with honors* in 1986 from George Washington University, where he was the Articles Editor of *The George Washington Journal of International Law and Economics*. He received his BA *magna cum laude* in economics and political science from Tufts University.

He may be contacted at iballon@manatt.com.